Lecture 6 – Hash functions

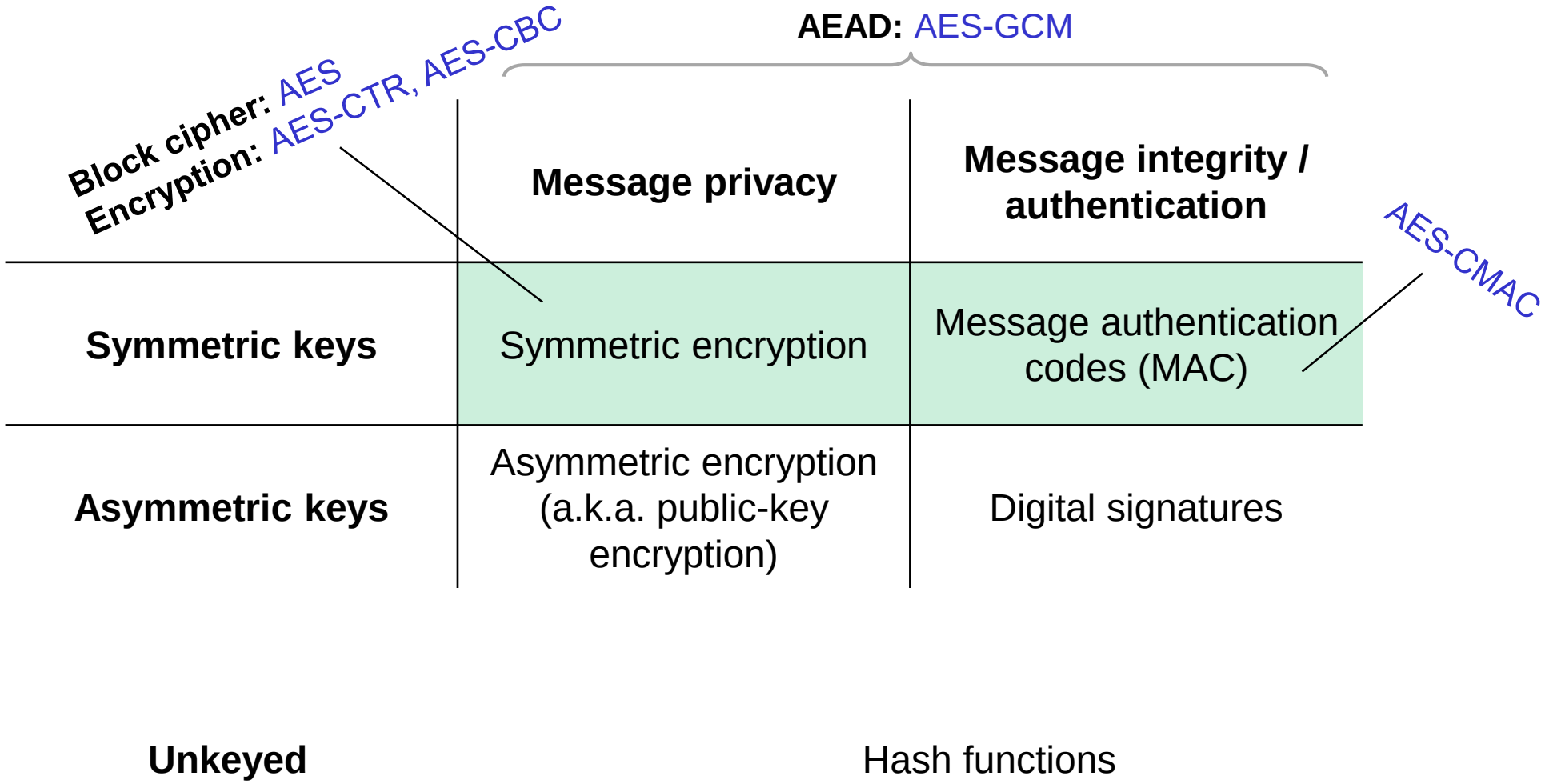
TEK4500

23.09.2026

Håkon Jacobsen

hakon.jacobsen@its.uio.no

Basic goals of cryptography



Hash function applications

- File storage verification
- Data authentication (MACs and digital signatures)
- Certificates
- Randomness extraction and key derivation (PRFs)
- Password hashing
- Quantum-resistant signatures
- Hash chains (Bitcoin)

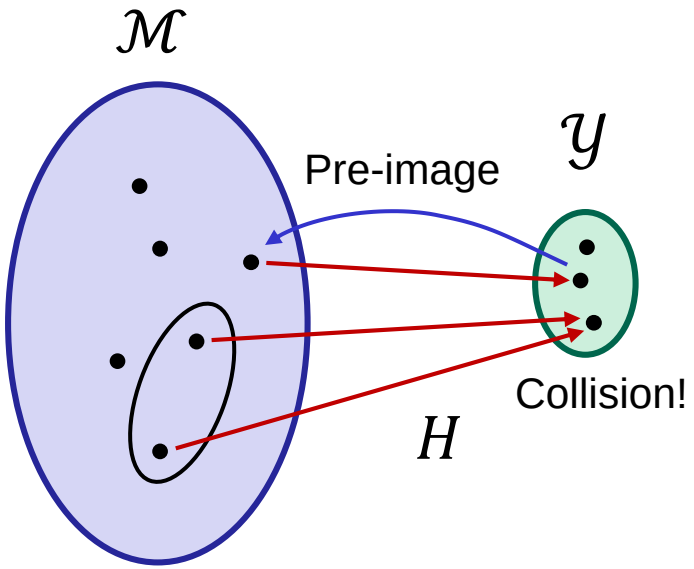
Hash functions

$H : \mathcal{M} \rightarrow \mathcal{Y}$

Keyless function

$|\mathcal{M}| \gg |\mathcal{Y}|$

Compressing



Examples:

- ~~$\mathrm{MD5} : \{0,1\}^* \rightarrow \{0,1\}^{128}$~~
- ~~$\mathrm{SHA1} : \{0,1\}^* \rightarrow \{0,1\}^{160}$~~
- $\mathrm{SHA2\text{-}256} : \{0,1\}^* \rightarrow \{0,1\}^{256}$
- $\mathrm{SHA2\text{-}512} : \{0,1\}^* \rightarrow \{0,1\}^{512}$

Possible security goals:

- Hard to find *pre-images*
- Hard to find *collisions*

Collision resistance

$\mathbf{Exp}_H^{\mathrm{cr}}(A)$

1. $(X, X') \leftarrow A$
2. **return** $H(X) \stackrel{?}{=} H(X')$ and $X \stackrel{?}{\neq} X'$

Intuition: H is **collision resistant** if $\mathbf{Adv}_H^{\mathrm{cr}}(A)$ is "*small*" for all "*practical*" A

Doesn't work!

There always *exists* a very efficient A with $\mathbf{Adv}_H^{\mathrm{cr}}(A) = 1$:

Since $|\mathcal{M}| > |\mathcal{Y}|$, there *exists* $X \neq X'$ s.t. $H(X) = H(X')$

A

1. Output X, X'

$\mathbf{Adv}_H^{\mathrm{cr}}(A) = 1$

…but how do we actually *find* X, X'?

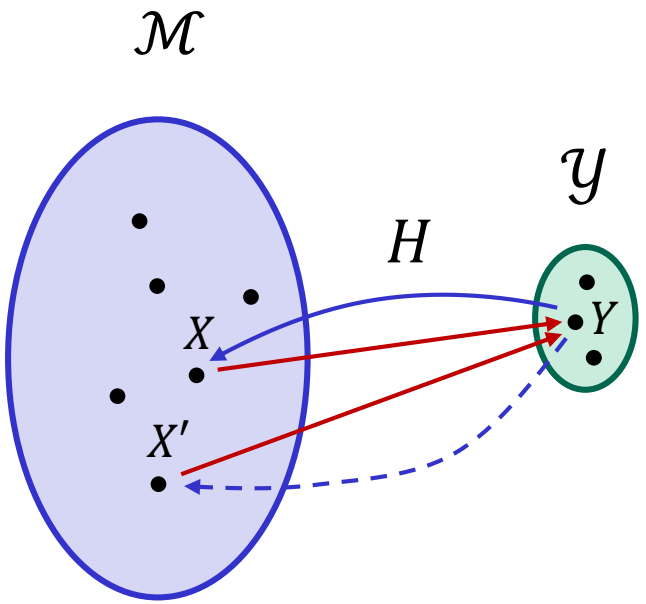
Definition: The **CR-advantage** of an adversary A against H is

$$\mathbf{Adv}_H^{\mathrm{cr}}(A) = \Pr[\mathbf{Exp}_H^{\mathrm{cr}}(A) \Rightarrow 1]$$

One-way / pre-image security

$\mathbf{Exp}_H^{\mathrm{ow}}(A)$

1. $X \twoheadleftarrow \mathcal{M}$
2. $Y \leftarrow H(X)$
3. $X' \leftarrow A(Y)$
4. **return** $H(X') \stackrel{?}{=} Y$



Definition: The **OW-advantage** of an adversary A against H is

$$\mathbf{Adv}_H^{\mathrm{ow}}(A) = \Pr[\mathbf{Exp}_H^{\mathrm{cr}}(A) \Rightarrow 1]$$

Collision resistance vs. one-wayness

$\mathbf{Exp}_H^{\mathrm{cr}}(A)$

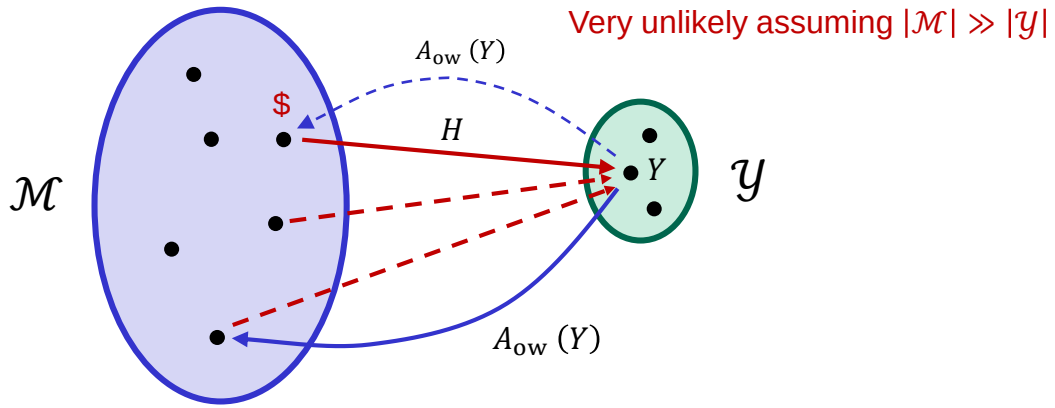
1. $(X, X') \leftarrow A$
2. **return** $H(X) \overset{?}{=} H(X')$ and $X \overset{?}{\neq} X'$

$\mathbf{Exp}_H^{\mathrm{ow}}(A)$

1. $X \twoheadleftarrow \mathcal{M}$
2. $Y \leftarrow H(X)$
3. $X' \leftarrow A(Y)$
4. **return** $H(X') \overset{?}{=} Y$

Theorem: Collision-resistance $\Longrightarrow$ One-wayness

Proof (sketch): suppose A_{ow} breaks one-wayness



Collision resistance vs. one-wayness

$\mathbf{Exp}_H^{\mathrm{cr}}(A)$

1. $(X, X') \leftarrow A$
2. **return** $H(X) \overset{?}{=} H(X')$ and $X \overset{?}{\neq} X'$

$\mathbf{Exp}_H^{\mathrm{ow}}(A)$

1. $X \twoheadleftarrow \mathcal{M}$
2. $Y \leftarrow H(X)$
3. $X' \leftarrow A(Y)$
4. **return** $H(X') \overset{?}{=} Y$

Theorem: Collision-resistance $\Longrightarrow$ One-wayness

Theorem: Collision-resistance $\not\Longleftarrow$ One-wayness

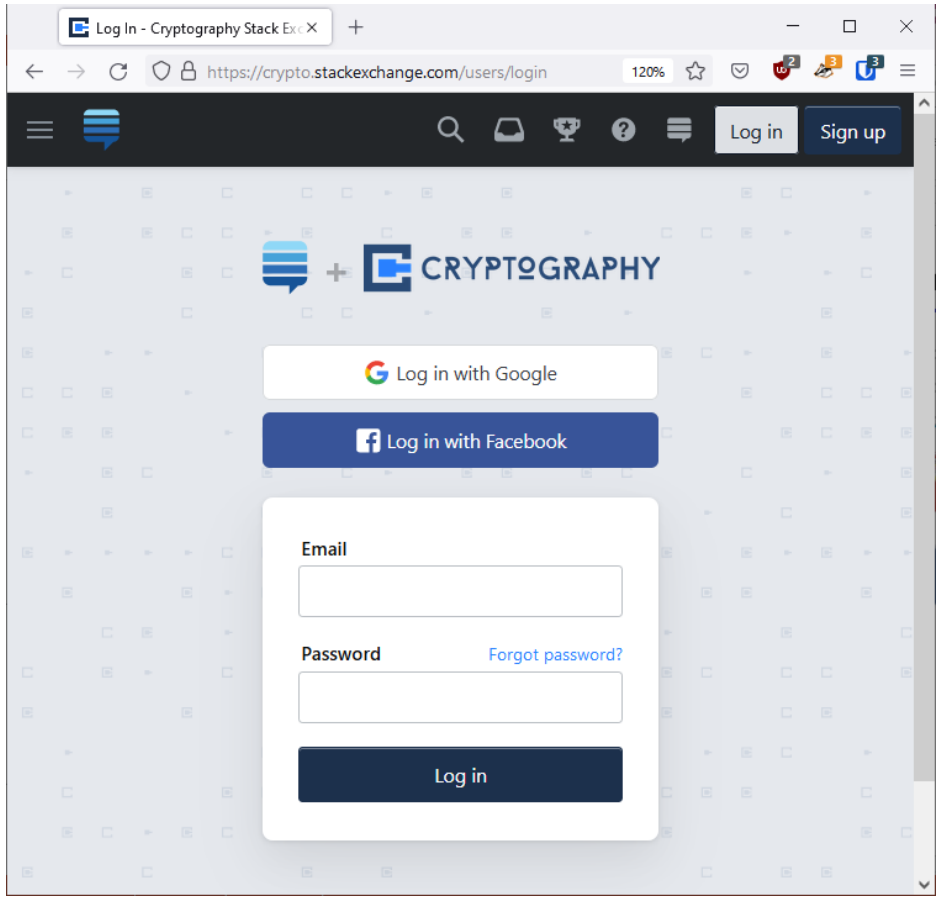
Suppose $H : \mathcal{M} \to \{0,1\}^{256}$ is one-way. Define:

$$H'(X) = \begin{cases} 0^{256} & \text{if } X \in \{00,11\} \\ H(X) & \text{otherwise} \end{cases}$$

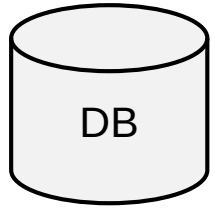
H' is one-way (if $|\mathcal{M}|$ is large)

H' is **not** collision-resistant

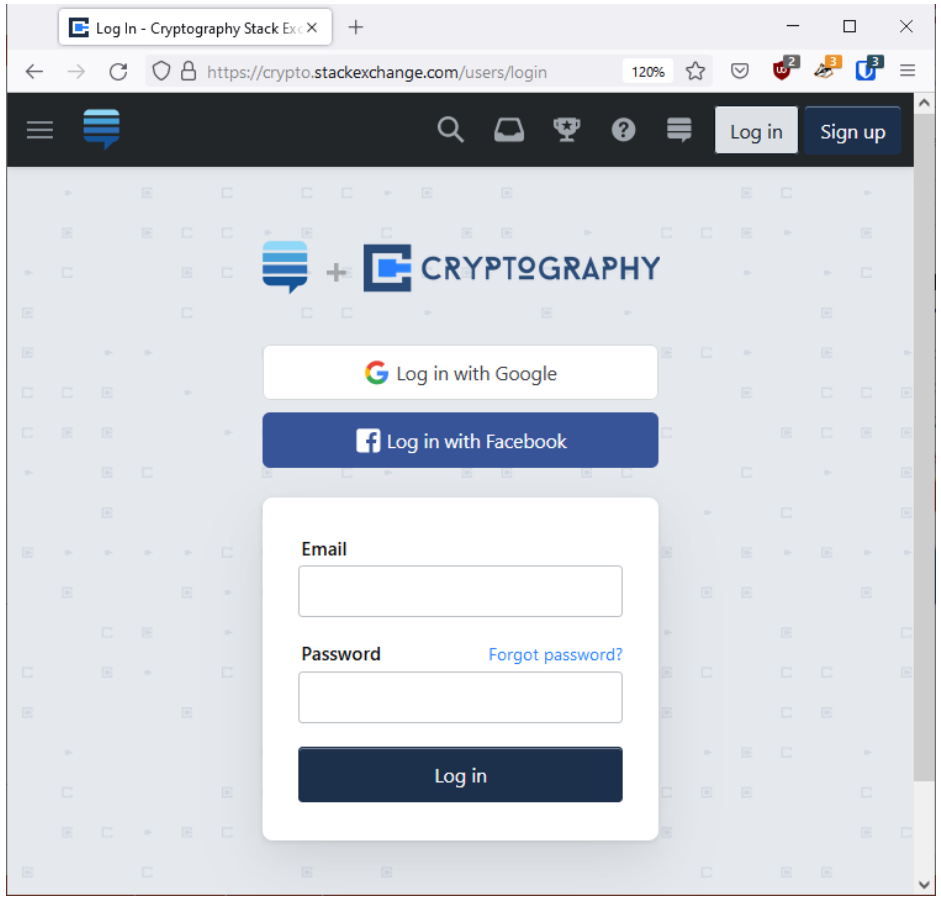
Hash function applications – password storage



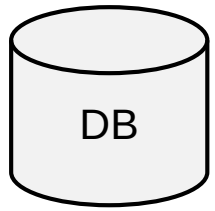
Username	Password
Alice	cat
Bob	dog
Charlie	pwd1234
Dave	batman
Eve	dog
…	…



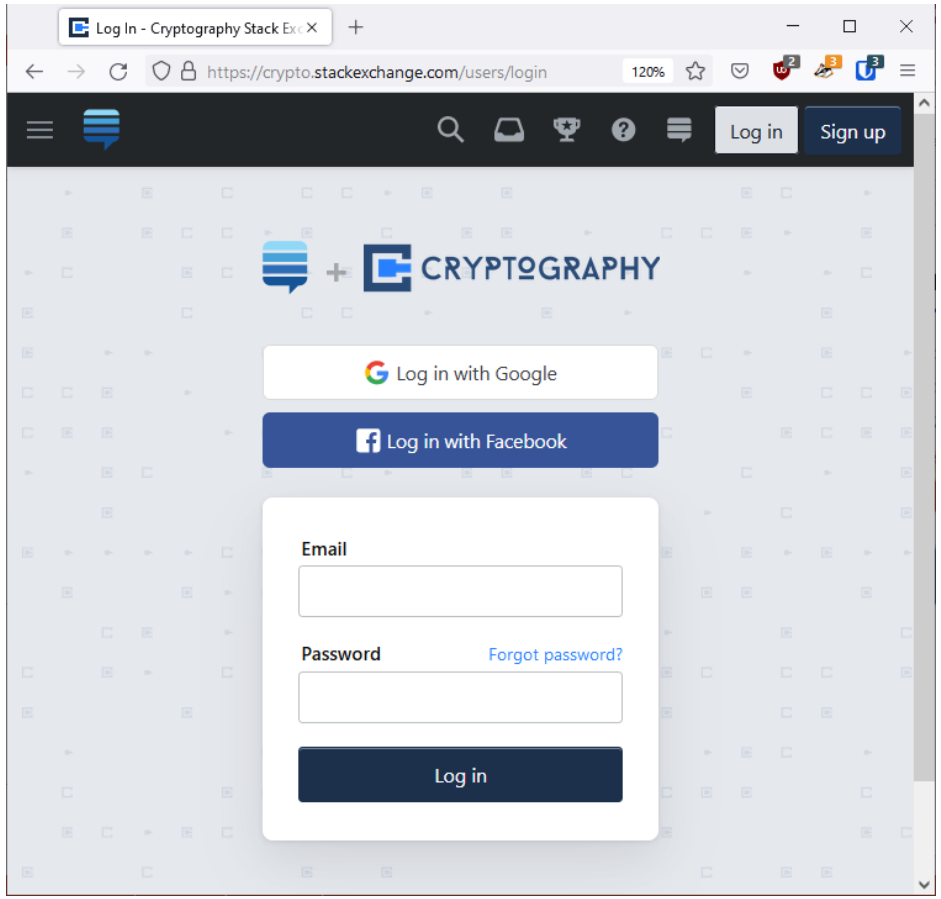
Hash function applications – password storage



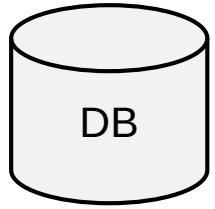
Username	Password
Alice	H(cat)
Bob	H(dog)
Charlie	H(pwd1234)
Dave	H(batman)
Eve	H(dog)
…	…



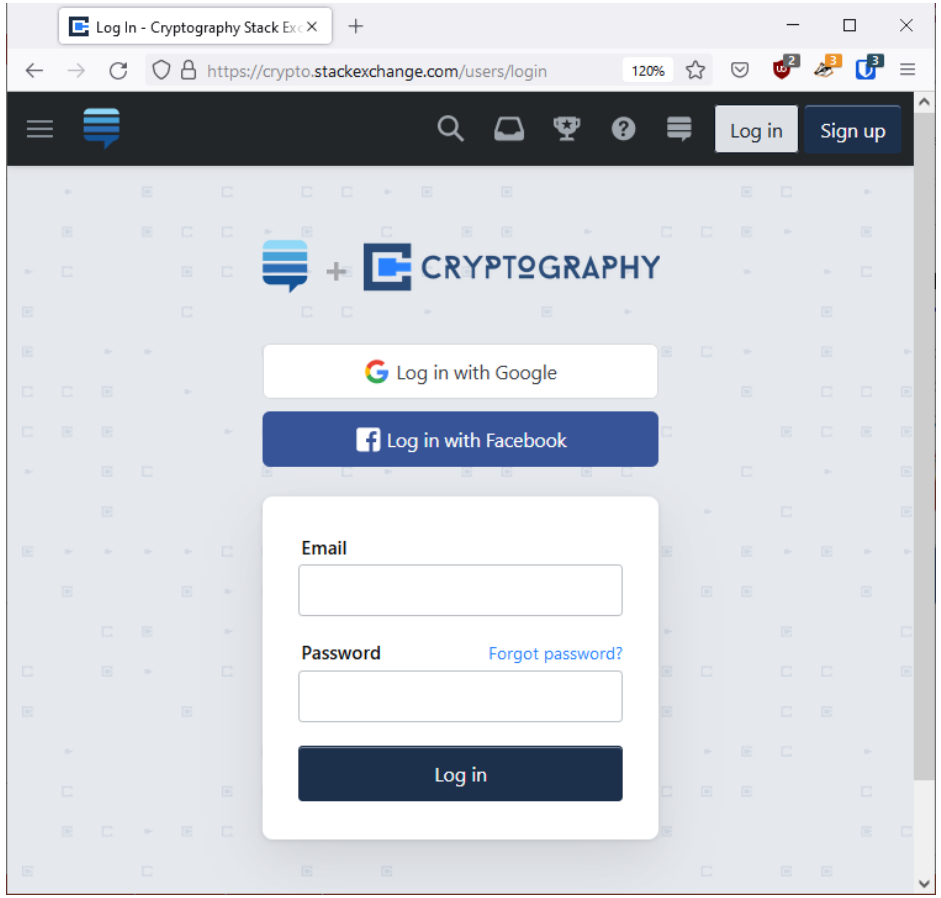
Hash function applications – password storage



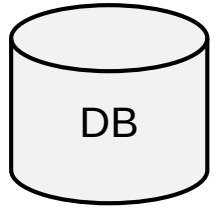
Username	Password
Alice	0x1b383a798bc2c5
Bob	0x512df2a1e63860
Charlie	0x26c540082d18cd
Dave	0xe33805da40919f
Eve	0x512df2a1e63860
…	…



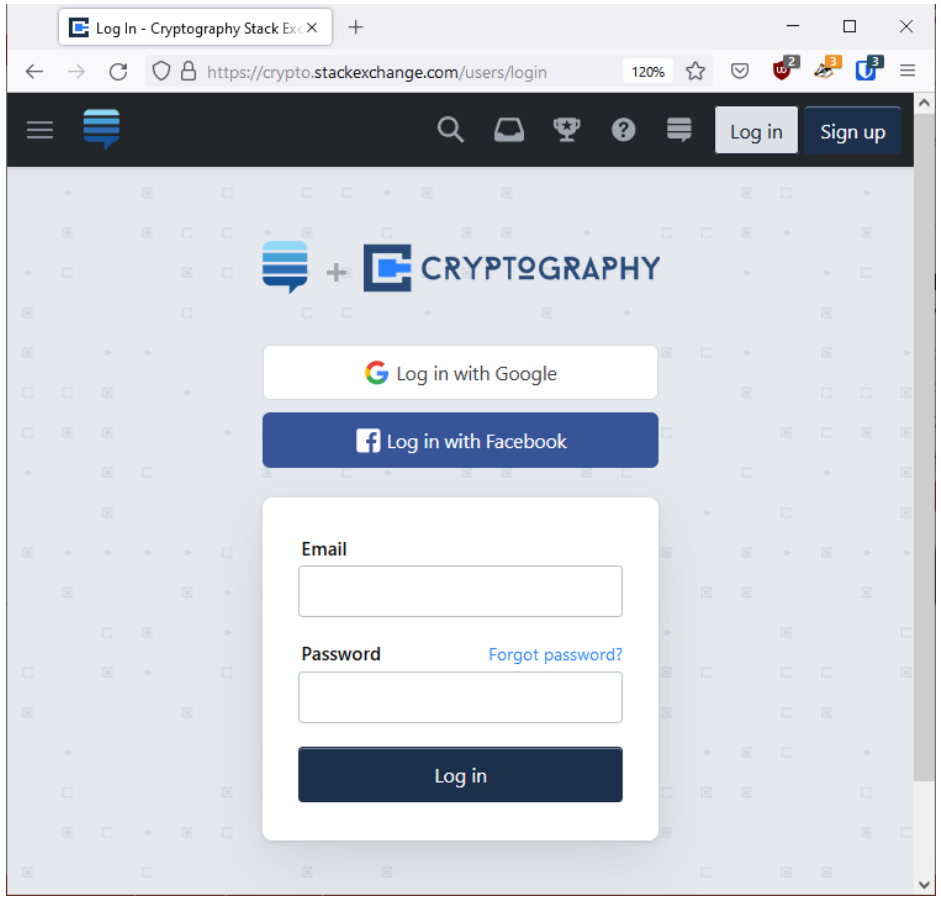
Hash function applications – password storage



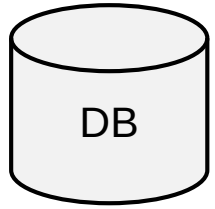
Username	Salt	Password
Alice	s1	H(s1,cat)
Bob	s2	H(s2,dog)
Charlie	s3	H(s3,pwd1234)
Dave	s4	H(s4,batman)
Eve	s5	H(s5,dog)
…	…	…



Hash function applications – password storage



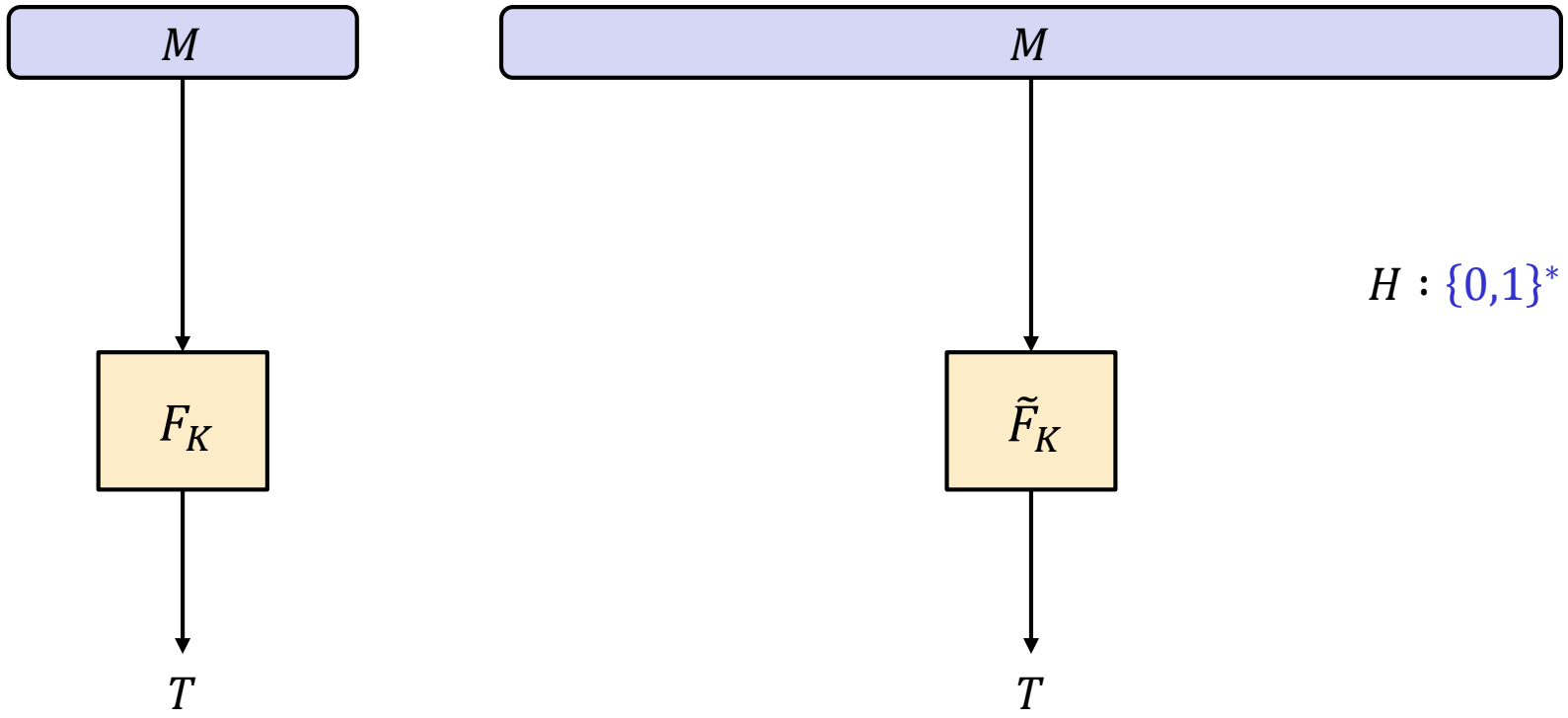
Username	Password
Alice	0x1b383a798bc2c5
Bob	0x512df2a1e63860
Charlie	0x26c540082d18cd
Dave	0xe33805da40919f
Eve	0x77faa039100423
…	…



Hash function applications – variable-input-length PRFs

$F : \mathcal{K} \times \{0,1\}^{in} \rightarrow \{0,1\}^{out}$

$\tilde{F} : \mathcal{K} \times \{0,1\}^{*} \rightarrow \{0,1\}^{out}$

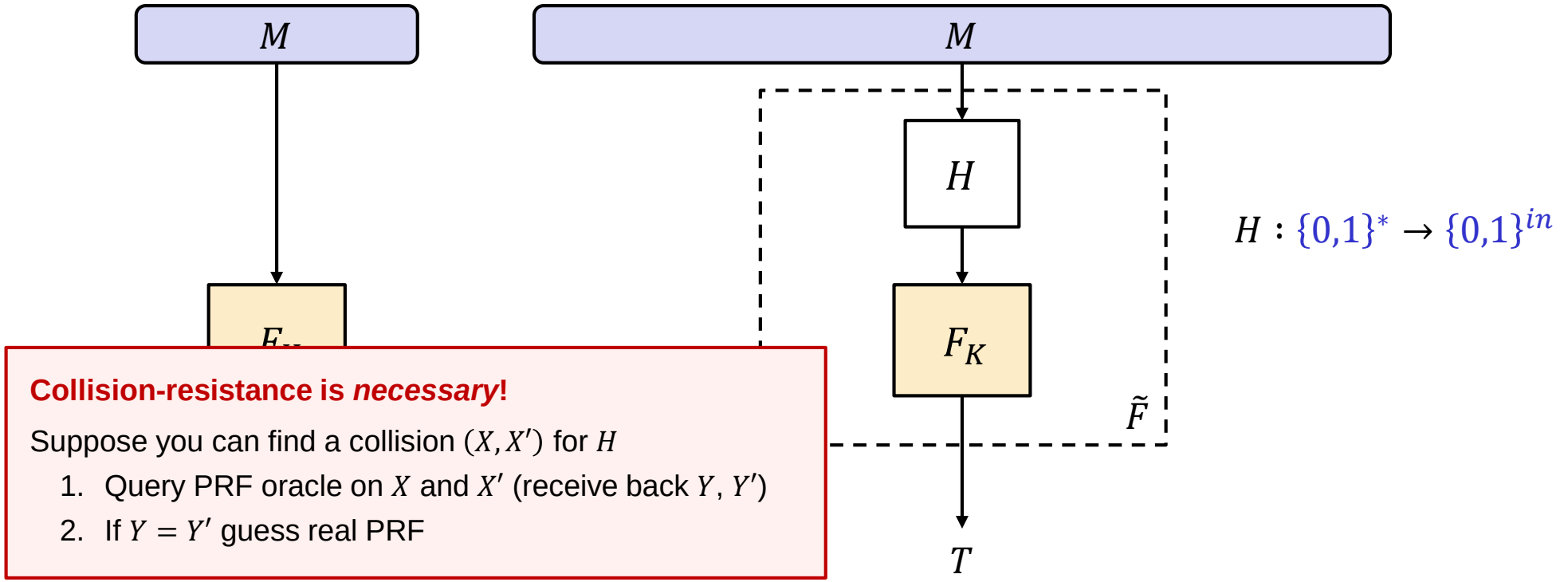


$H : \{0,1\}^{*} \rightarrow \{0,1\}^{in}$

Hash function applications – variable-input-length PRFs

$F : \mathcal{K} \times \{0,1\}^{in} \to \{0,1\}^{out}$

$\tilde{F} : \mathcal{K} \times \{0,1\}^{*} \to \{0,1\}^{out}$



Collision-resistance is *necessary*!

Suppose you can find a collision (X, X') for H

1. Query PRF oracle on X and X' (receive back Y, Y')
2. If $Y = Y'$ guess real PRF

Theorem: H is collision resistant and F is a secure PRF $\Longrightarrow$ $\tilde{F}$ is a secure VIL-PRF

Hash function applications – commitment schemes









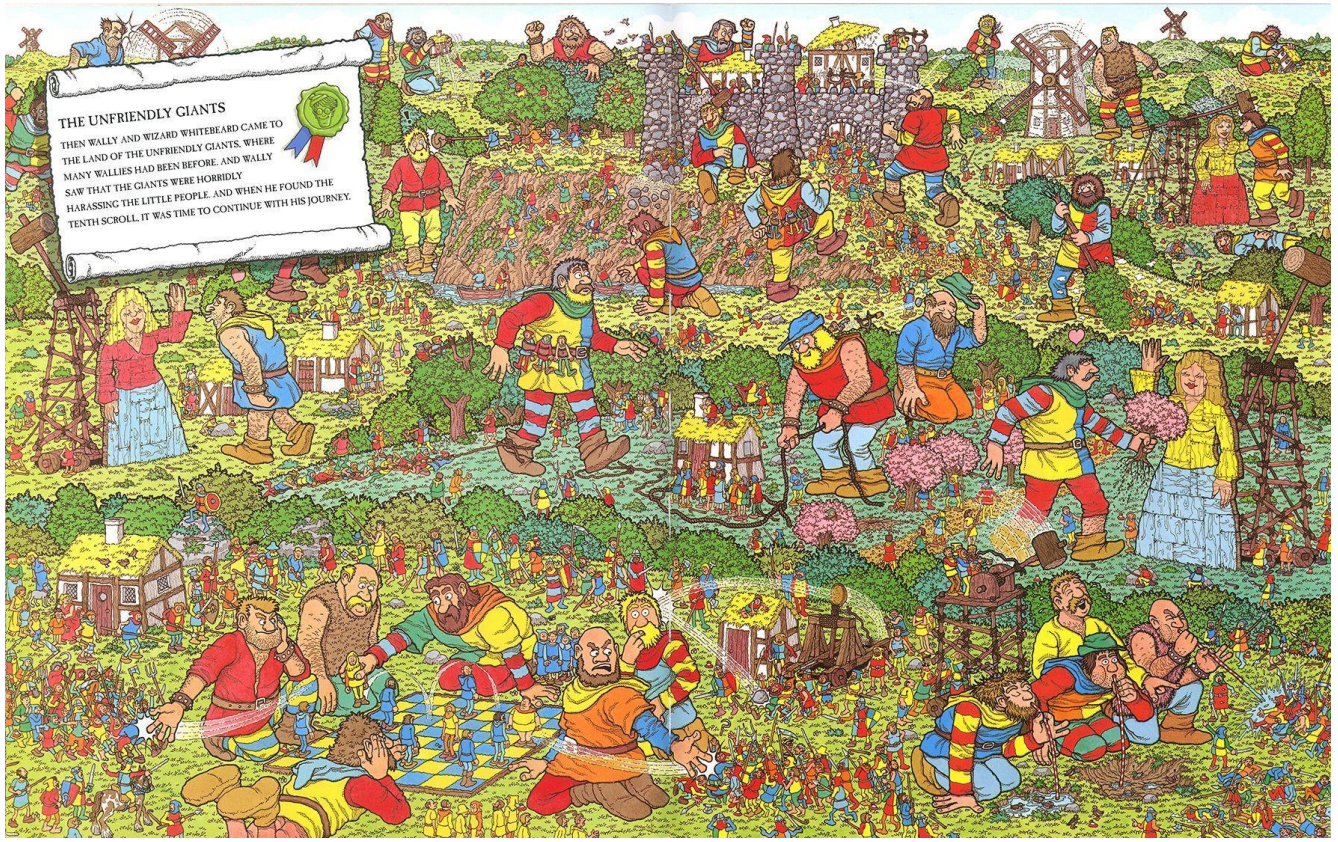




Hash function applications – commitment schemes



"Bob: Waldo is at pos. …" → H → `0x59d67`



"Alice: Waldo is at pos. …"

H



`0x4fb04`

"Charlie: Waldo is at pos. …"



H

`0xf2200`

Attacks on hash functions

- Specific attacks: exploit **internal design** of hash function

- Generic attacks: work **for all** hash functions $H : \{0,1\}^* \rightarrow \{0,1\}^n$

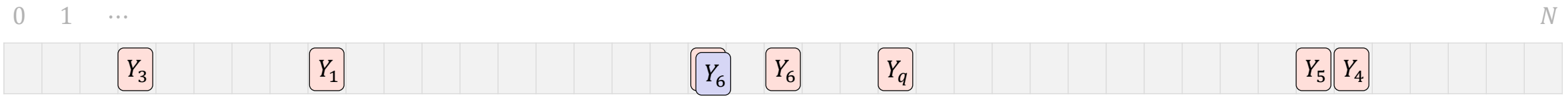
  - Brute-force: hash $\mathbf{1}, \mathbf{2}, \mathbf{3}, \ldots, \mathbf{2^n + 1}$ $\mathbf{Adv}_H^{cr}(A) = 1$
    - Output must be long enough
      $n = 10$ requires only $2^{10} + 1 = 1025$ values
    - $n = 100$ enough?

  - Brute-force 2: hash $\mathbf{1}, \mathbf{2}, \mathbf{3}, \ldots, \boldsymbol{q}$ $\mathbf{Adv}_H^{cr}(B) \approx 1$ $q \approx 2^{50} \ll 2^{100}$



The birthday paradox

Birthday attack



$Y_1 \leftarrow H(X_1)$

$Y_2 \leftarrow H(X_2)$

$Y_3 \leftarrow H(X_3)$

$Y_4 \leftarrow H(X_4)$

$Y_5 \leftarrow H(X_5)$

$Y_6 \leftarrow H(X_6)$

$\vdots$

$Y_q \leftarrow H(X_q)$

$$\mathbf{Adv}_H^{\mathrm{cr}}(B) = \Pr[\mathrm{coll}] = \Pr\left[\exists i \neq j : H(X_i) = H(X_j)\right]$$

Birthday attack



$Y_1 \twoheadleftarrow \mathcal{Y}$

$Y_2 \twoheadleftarrow \mathcal{Y}$

$Y_3 \twoheadleftarrow \mathcal{Y}$

$Y_4 \twoheadleftarrow \mathcal{Y}$

$Y_5 \twoheadleftarrow \mathcal{Y}$

$Y_6 \twoheadleftarrow \mathcal{Y}$

$\vdots$

$Y_q \twoheadleftarrow \mathcal{Y}$

$$\mathbf{Adv}^{\mathrm{cr}}_H(B) = \Pr[\mathrm{coll}] = \Pr\left[\exists i \neq j : H(X_i) = H(X_j)\right]$$

Birthday attack



$$\Pr[\text{coll}] = 1 - \Pr[\text{no-coll}] \geq 1 - e^{-\frac{q(q-1)}{2N}}$$

$$\Pr[\text{no-coll}] = 1 \times \frac{N-1}{N} \times \frac{N-2}{N} \times \frac{N-3}{N} \quad \cdots \quad \times \frac{N-(q-1)}{N}$$

$$(1-x) \leq e^{-x} \qquad x \geq 0$$

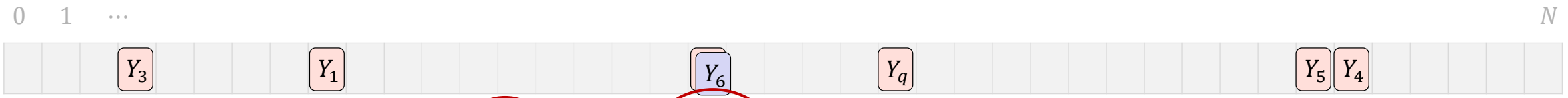
$$= 1 \times \left(1 - \frac{1}{N}\right) \times \left(1 - \frac{2}{N}\right) \times \left(1 - \frac{3}{N}\right) \cdots \times \left(1 - \frac{q-1}{N}\right)$$

$$e^{-x} = 1 - \frac{x}{1!} + \underbrace{\frac{x^2}{2!} - \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots}_{> 0}$$

$$\leq 1 \cdot e^{-1/N} \cdot e^{-2/N} \cdot e^{-3/N} \quad \cdots \quad e^{-(q-1)/N}$$

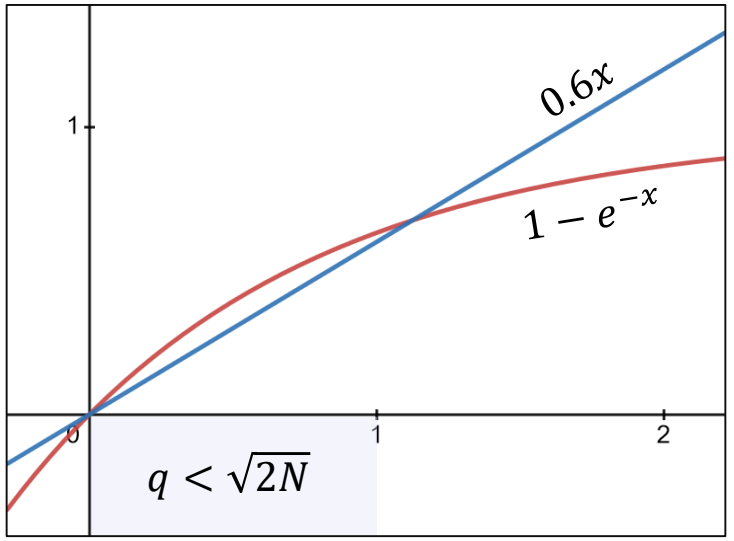
$$= e^{-(1+2+\cdots+q-1)/N} = e^{-\frac{q(q-1)}{2N}}$$

Birthday attack



$$\Pr[\text{coll}] = 1 - \Pr[\text{no-coll}] \geq 1 - e^{-\frac{q(q-1)}{2N}} \geq 0.6 \times \frac{q(q-1)}{2N}$$

x



Birthday attack



$$0.6 \times \frac{q(q-1)}{2N} \leq \Pr[\text{coll}] = \Pr[\text{coll}_1 \vee \text{coll}_2 \vee \cdots \vee \text{coll}_q]$$

$$\leq \Pr[\text{coll}_1] + \Pr[\text{coll}_2] + \cdots + \Pr[\text{coll}_q]$$

$$\leq \frac{0}{N} + \frac{1}{N} + \cdots + \frac{q-1}{N}$$

$$= \frac{q(q-1)}{2N}$$

Birthday attack



$$0.6 \times \frac{q(q-1)}{2N} \leq \Pr[\text{coll}] \leq \frac{q(q-1)}{2N}$$

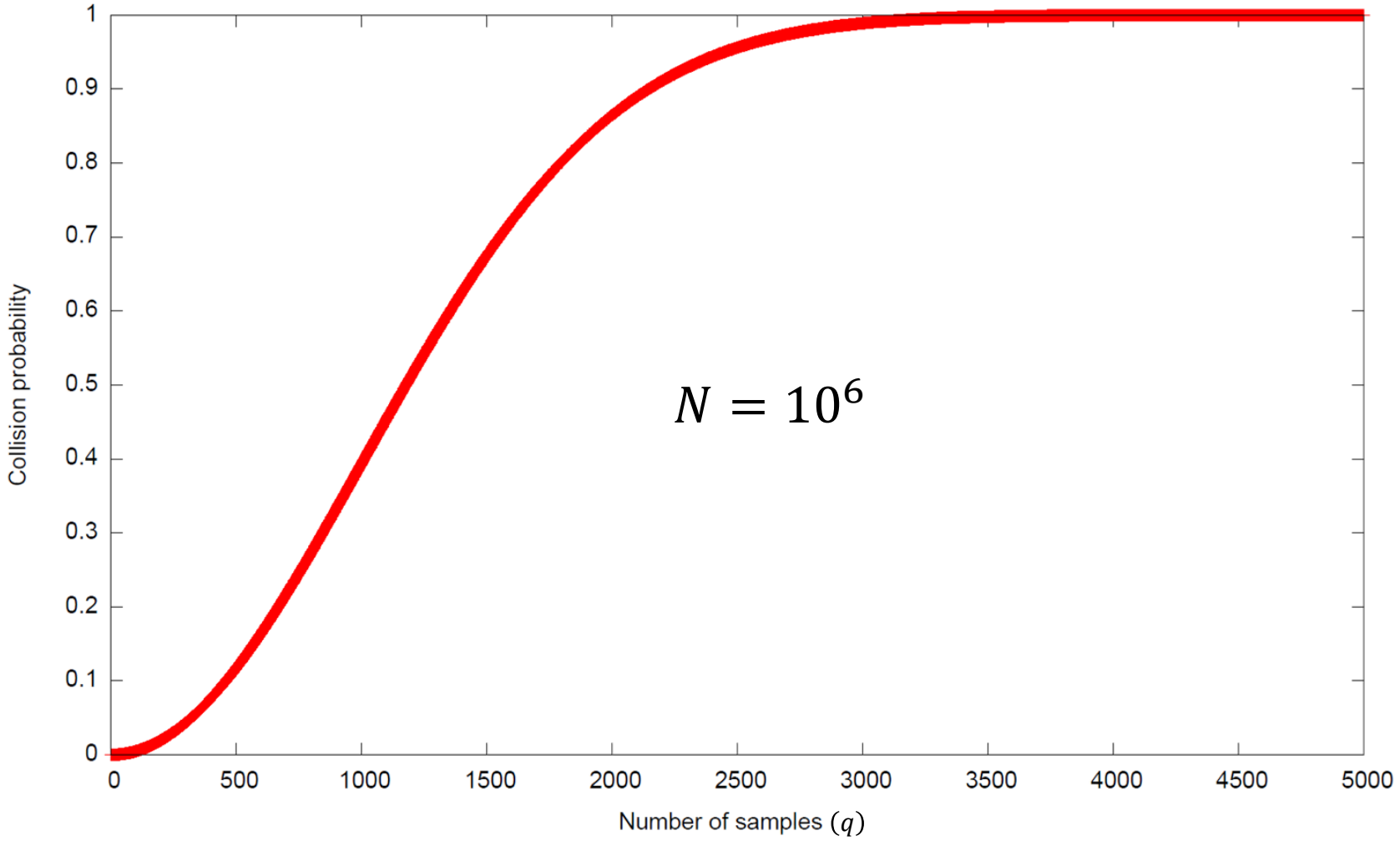
$\Pr[\text{coll}] = 0.5$:

$$q \approx \sqrt{N}$$

N	q
365	23
10^6	10^3
2^{64}	2^{32}
2^{80}	2^{40}
2^{256}	2^{128}
2^{512}	2^{256}

Birthday bound: For $q \leq \sqrt{2N}$ values drawn at random from $\{1,2,\ldots,N\}$

$$\Pr[\text{coll}] \approx \frac{q^2}{2N}$$


Collision probability
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
500
1000
1500
2000
2500
3000
3500
4000
4500
5000
Number of samples (q)
$N = 10^6$

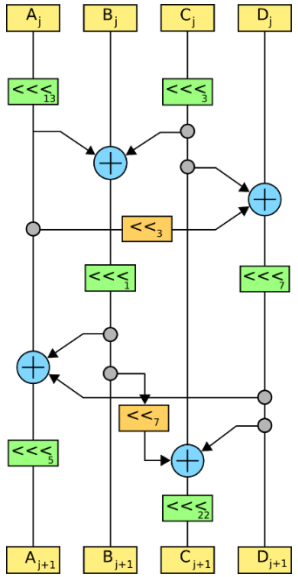
Attacks on hash functions

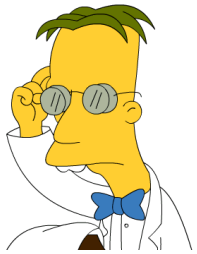
- Specific attacks: exploit **internal design** of hash function

- Generic attacks: work **for all** hash functions $H : \{0,1\}^* \rightarrow \{0,1\}^n$

  - Brute-force: hash $\mathbf{1}, \mathbf{2}, \mathbf{3}, \ldots, \mathbf{2^n + 1}$ $\mathbf{Adv}^{\mathrm{cr}}_H(A) = 1$
    - Output must be long enough
      $n = 10$ requires only $2^{10} + 1 = 1025$ values
    - $n = 100$ enough? No! $\boldsymbol{n/2}$ must be large enough $\Rightarrow$ $\boldsymbol{n \geq 200}$

  - Brute-force 2: hash $\mathbf{1}, \mathbf{2}, \mathbf{3}, \ldots, \boldsymbol{q}$ $\mathbf{Adv}^{\mathrm{cr}}_H(B) \approx 1$ $q \approx 2^{50} \ll 2^{100}$





Designing hash functions

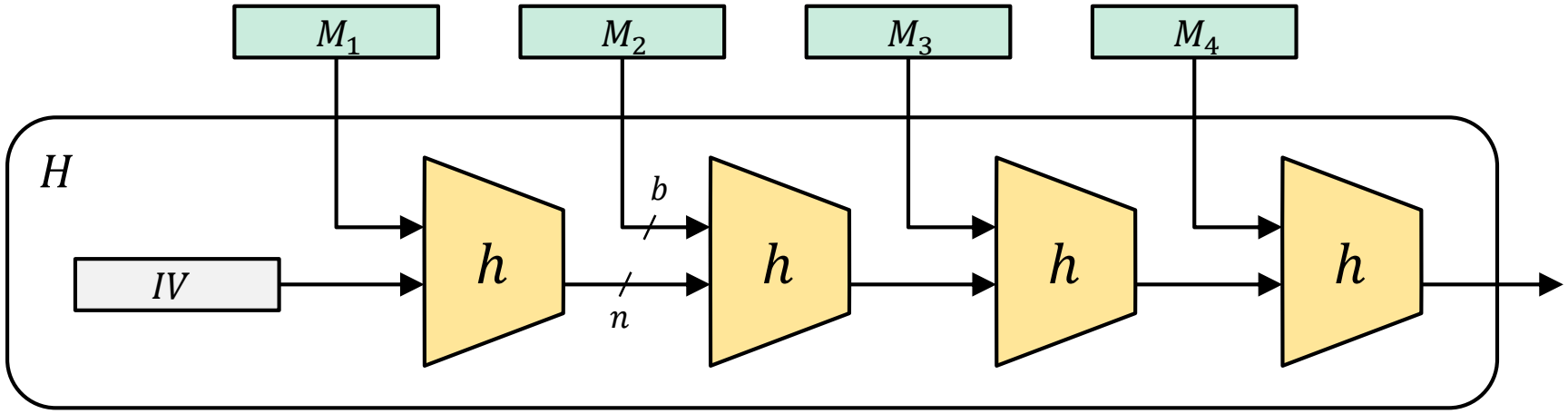
Merkle-Damgård

- Want to create a hash function $H : \{0,1\}^* \rightarrow \{0,1\}^n$
- Suppose we have a **compression function** $h : \{0,1\}^{n+b} \rightarrow \{0,1\}^n$ which is collision-resistant
- Solution: iterate h

Merkle-Damgård

$H : \{0,1\}^* \rightarrow \{0,1\}^n$

$$H(M) = h(h(\cdots h(h(IV, M_1), M_2) \cdots, M_{n-1}), M_n)$$

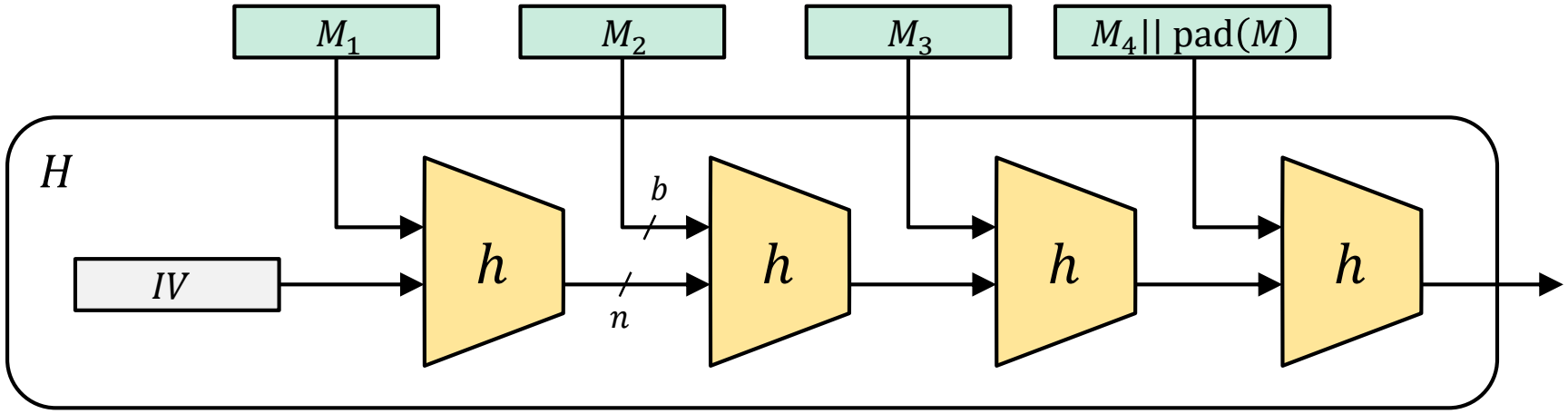


$h : \{0,1\}^{n+b} \rightarrow \{0,1\}^n$

Merkle-Damgård

$H : \{0,1\}^* \rightarrow \{0,1\}^n$

$$H(M) = h(h(\cdots h(h(IV, M_1), M_2) \cdots, M_{n-1}), M_n)$$

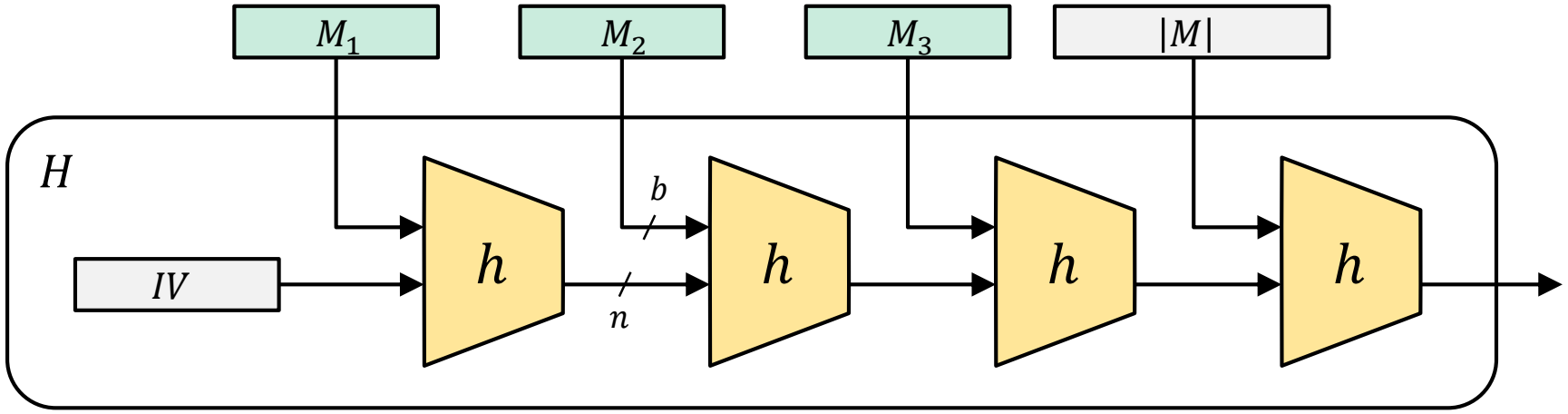


$h : \{0,1\}^{n+b} \rightarrow \{0,1\}^n$

Merkle-Damgård

$H : \{0,1\}^* \rightarrow \{0,1\}^n$

$$H(M) = h(h(\cdots h(h(IV, M_1), M_2) \cdots, M_{n-1}), M_n)$$



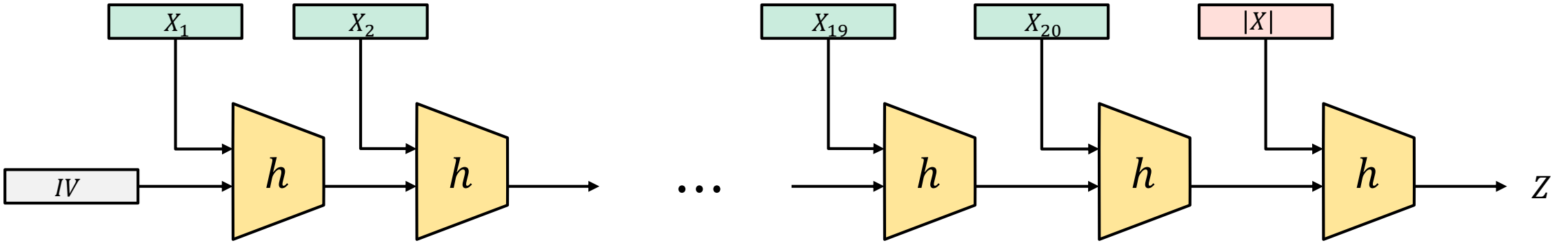
$h : \{0,1\}^{n+b} \rightarrow \{0,1\}^n$

Theorem: h is collision resistant $\Longrightarrow$ H is collision resistant

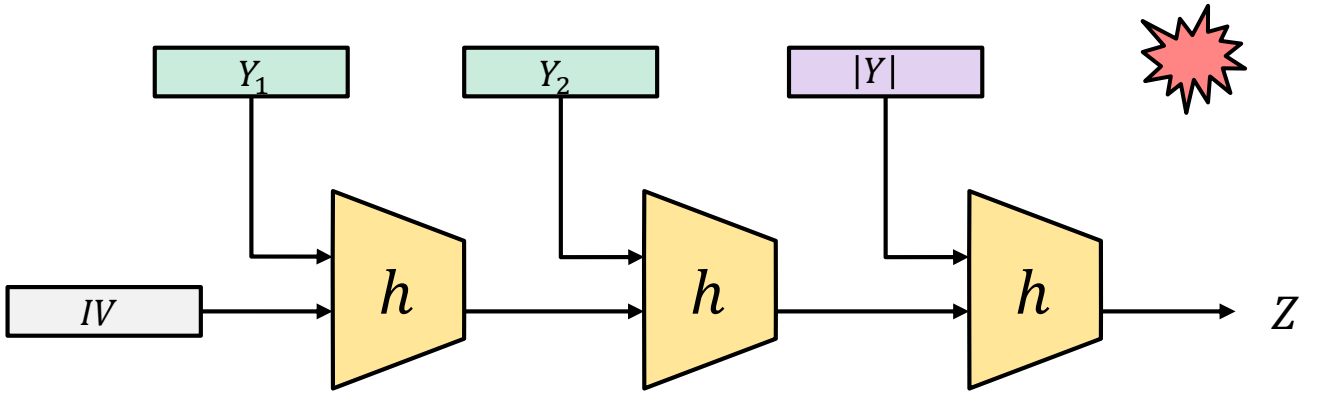
Proof idea: Collison for H $\Longrightarrow$ collision for h

Merkle-Damgård – security

Assumption: $X \neq Y$ and $H(X) = H(Y) = Z$

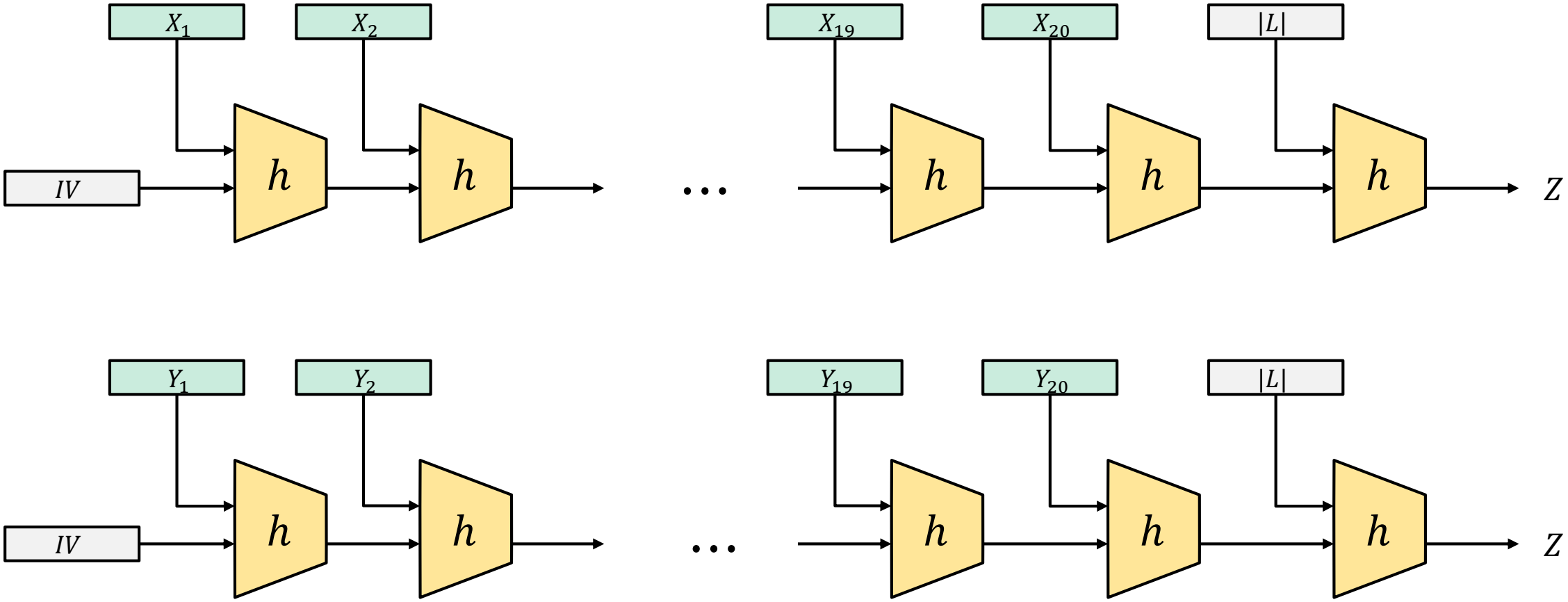


$h(*, |X|) = h(*, |Y|)$



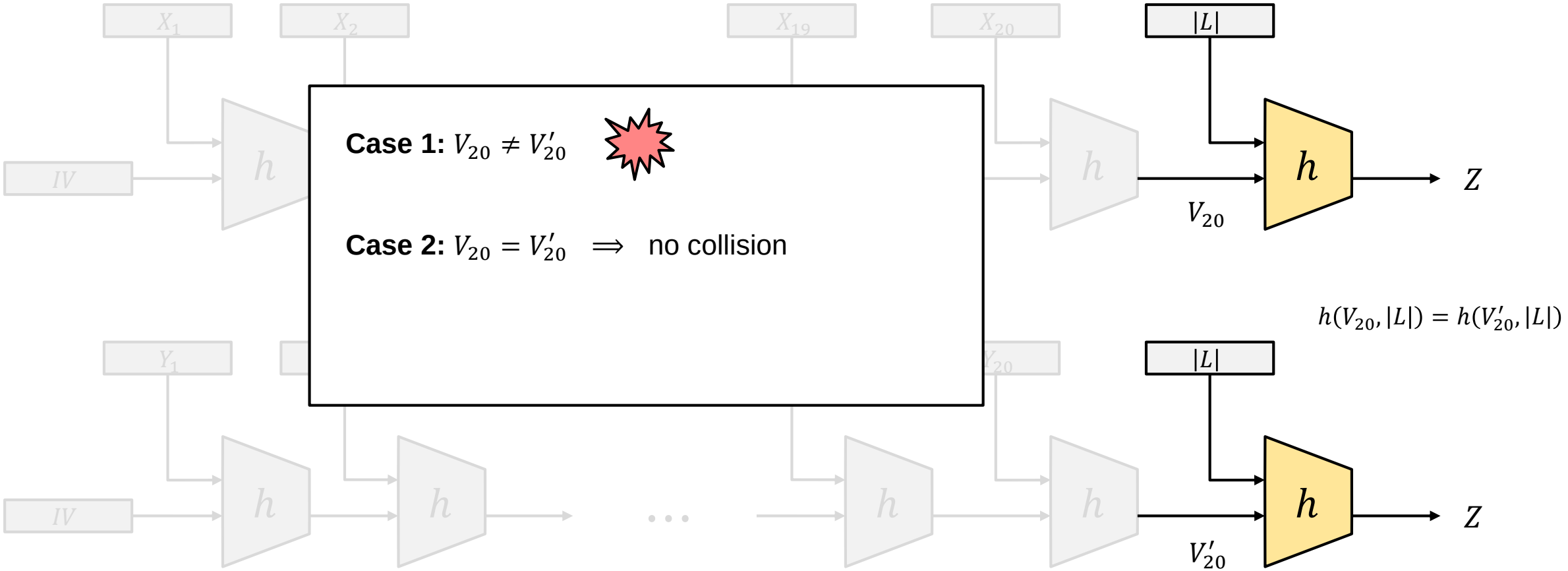
Merkle-Damgård – security

Assumption: $X \neq Y$ and $H(X) = H(Y) = Z$



Merkle-Damgård – security

Assumption: $X \neq Y$ and $H(X) = H(Y) = Z$

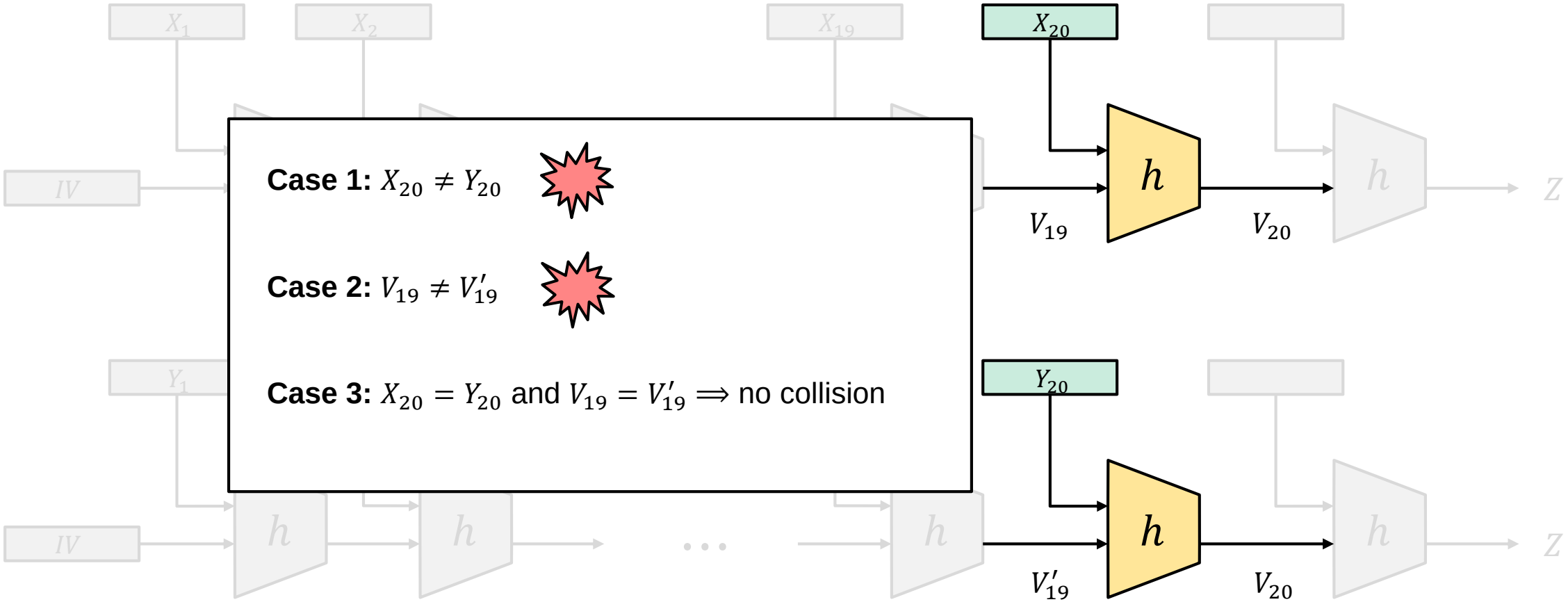


Case 1: $V_{20} \neq V'_{20}$

Case 2: $V_{20} = V'_{20} \implies$ no collision

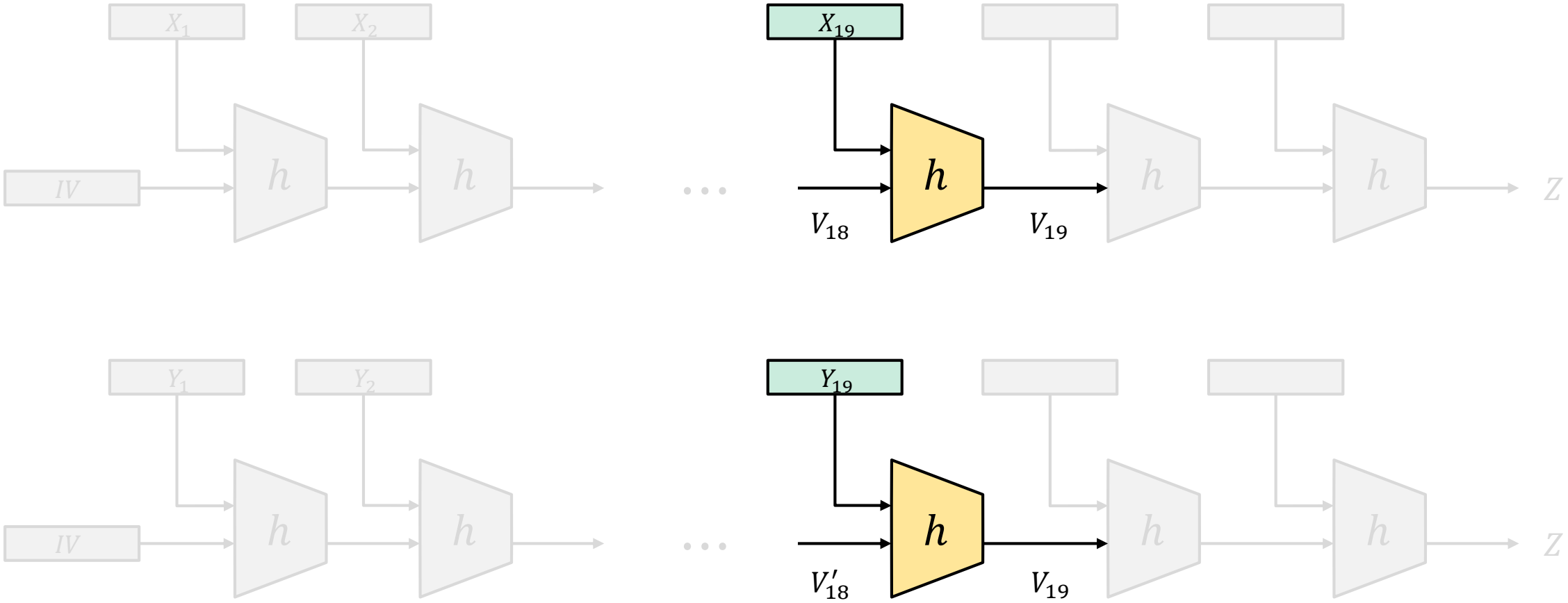
Merkle-Damgård – security

Assumption: $X \neq Y$ and $H(X) = H(Y) = Z$



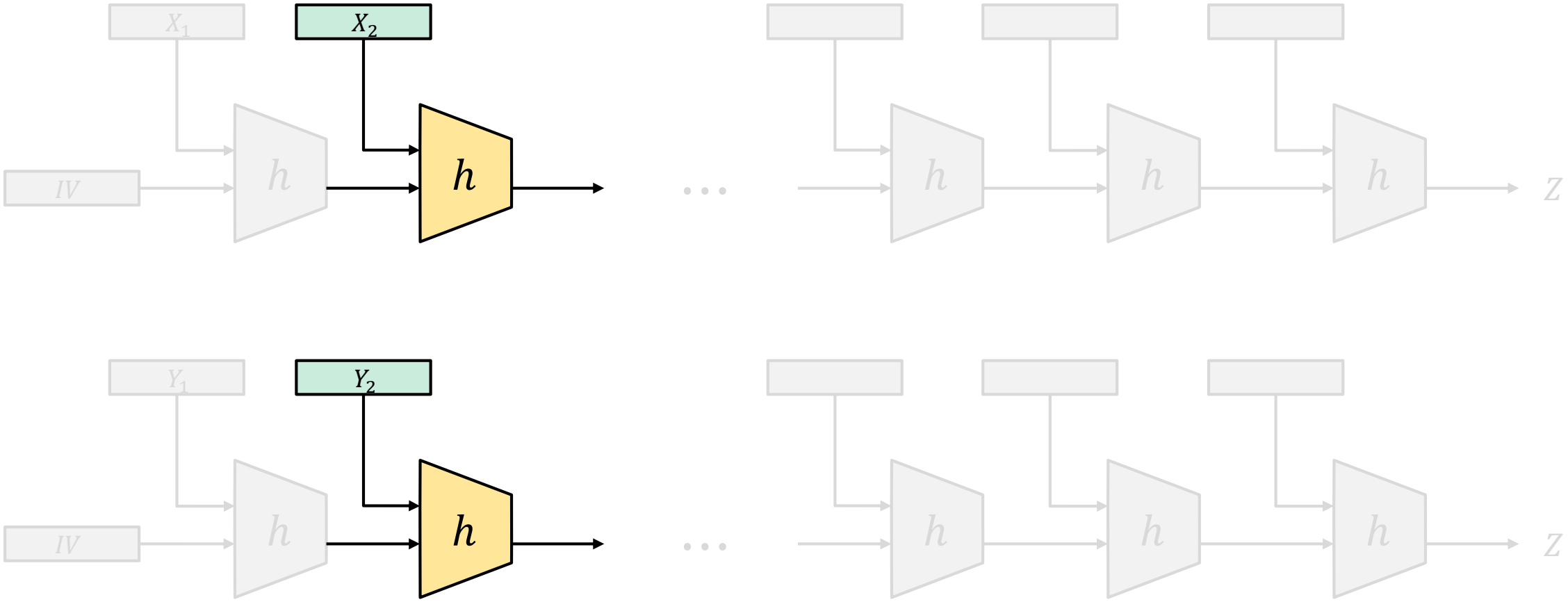
Merkle-Damgård – security

Assumption: $X \neq Y$ and $H(X) = H(Y) = Z$



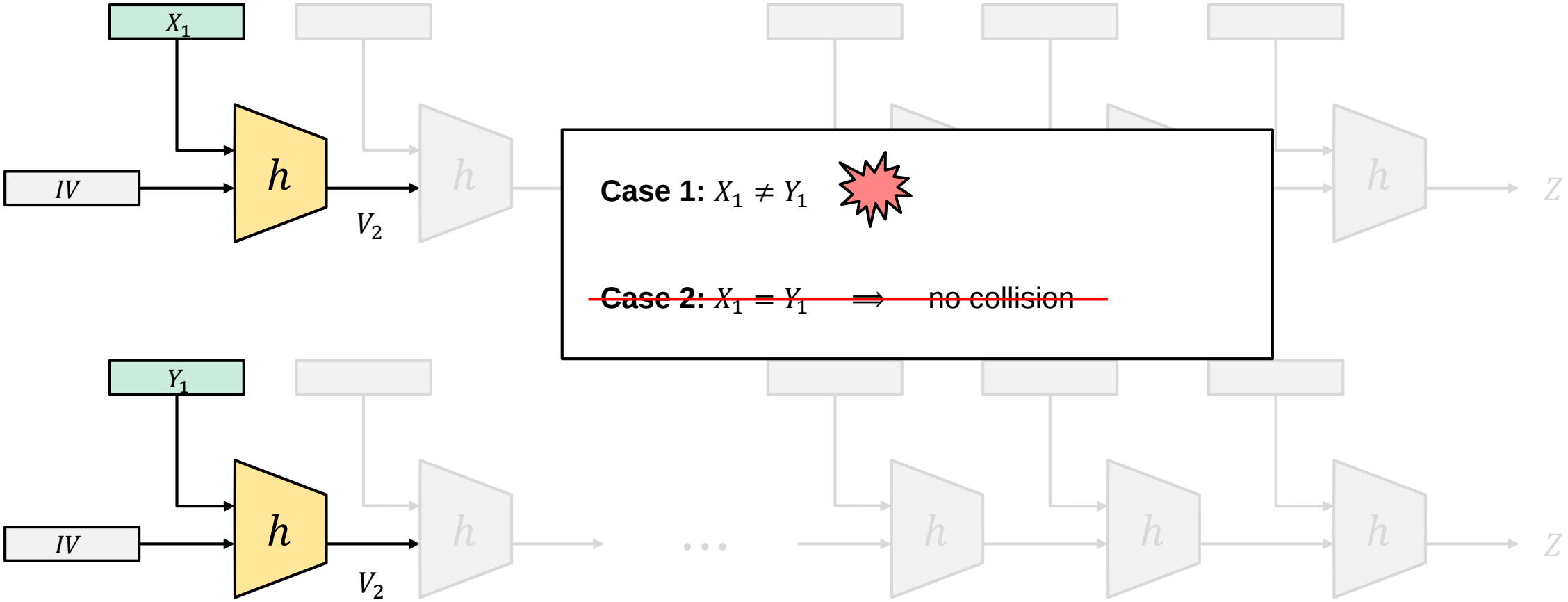
Merkle-Damgård – security

Assumption: $X \neq Y$ and $H(X) = H(Y) = Z$



Merkle-Damgård – security

Assumption: $X \neq Y$ and $H(X) = H(Y) = Z$

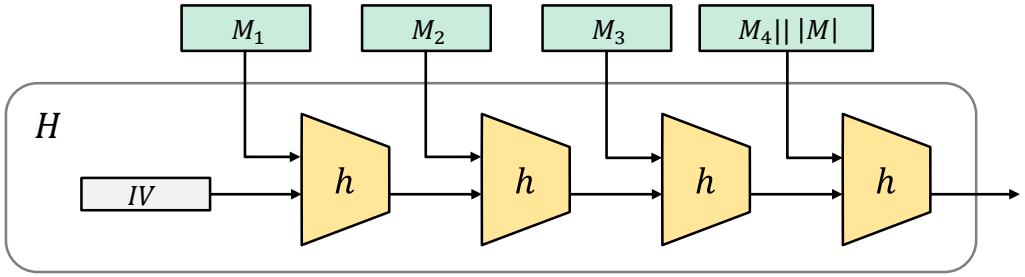


Compression function designs

- Merkle-Damgård creates collision resistant $H : \{0,1\}^* \rightarrow \{0,1\}^n$ from collision resistant $h : \{0,1\}^{b+n} \rightarrow \{0,1\}^n$

- Need only focus on compression function

$$h : \{0,1\}^{b+n} \rightarrow \{0,1\}^n$$

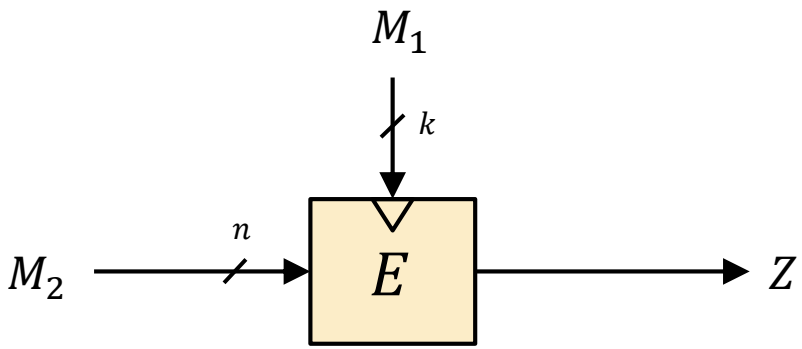


- Many design options for h
  - Ad-hoc
  - Structured

Compression functions from block ciphers – Davies-Meyer

$k+n \quad k \quad n$

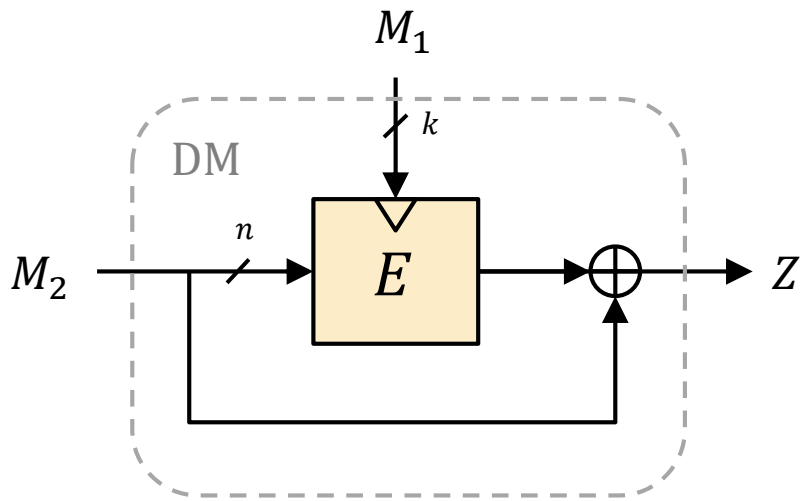
$M = M_1 \,||\, M_2$



Compression functions from block ciphers – Davies-Meyer

$k+n \quad k \quad n$

$M = M_1 \,||\, M_2$

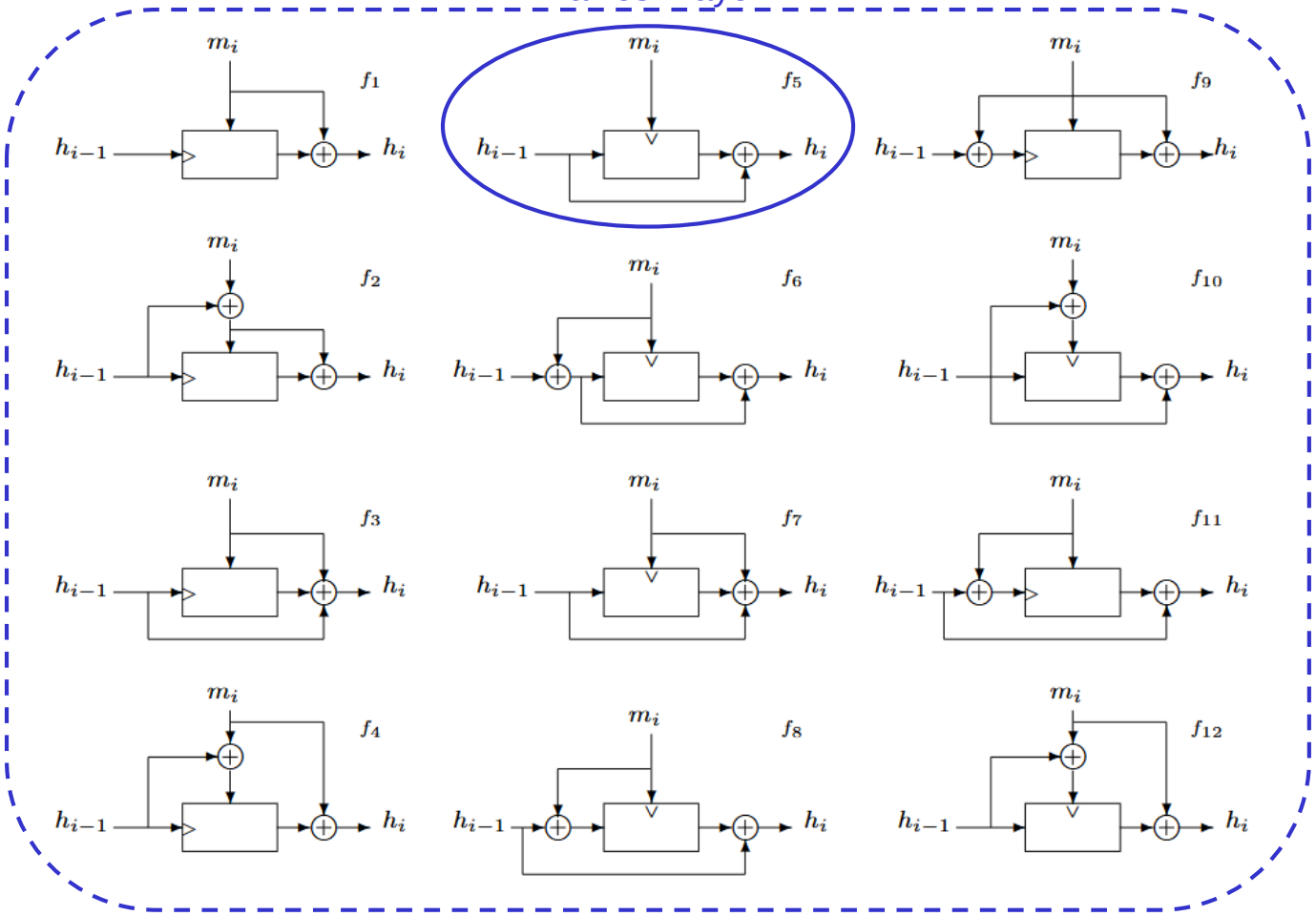


Warning! Not the same as the PRF/PRP setting

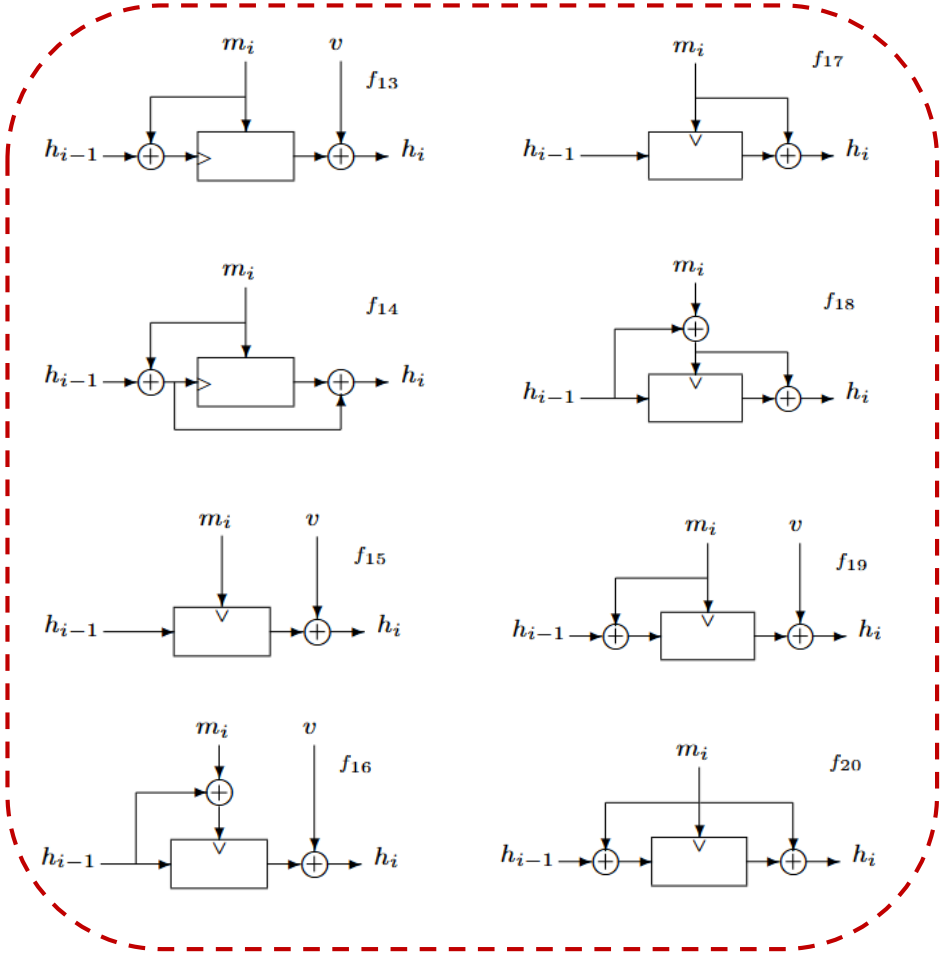
Theorem: $\mathrm{DM} : \{0,1\}^{k+n} \rightarrow \{0,1\}^n$ is a collision resistant compression function in the ***ideal cipher model***

Alternatives…

Davies-Mayer



Collision-resistant*



Not collision-resistant

Black, Rogaway & Shrimpton: Black-Box Analysis of the Block-Cipher-Based Hash-Function Constructions from PGV; CRYPTO'02

*In the ideal cipher model

SHA – Secure Hash Algorithm

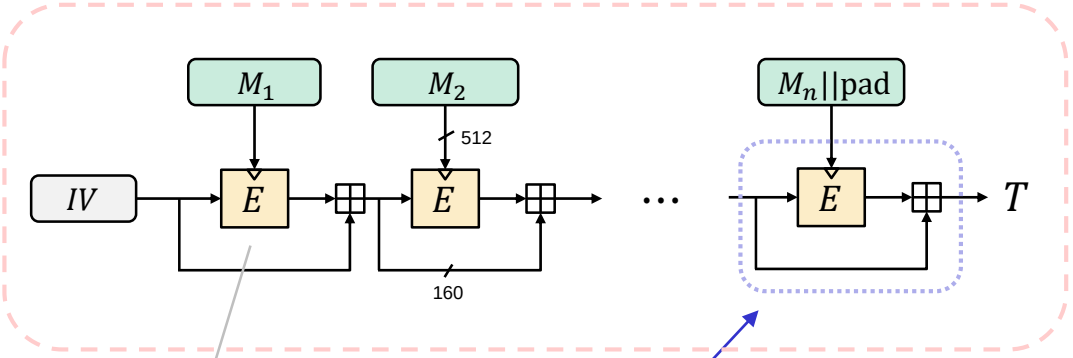
- Family of hash functions published by NIST
  - 1995: SHA1
  - 2001: SHA2-256 / SHA2-512
    - Also truncated versions: SHA2-224, SHA2-384
  - 2015: SHA3-256 / SHA3-512

- SHA1 and SHA2 designed by NSA
  - Merkle-Damgård + Davies-Meyer designs

- SHA3 designed by Belgian cryptographers
  - Sponge design

SHA1

Merkle-Damgård



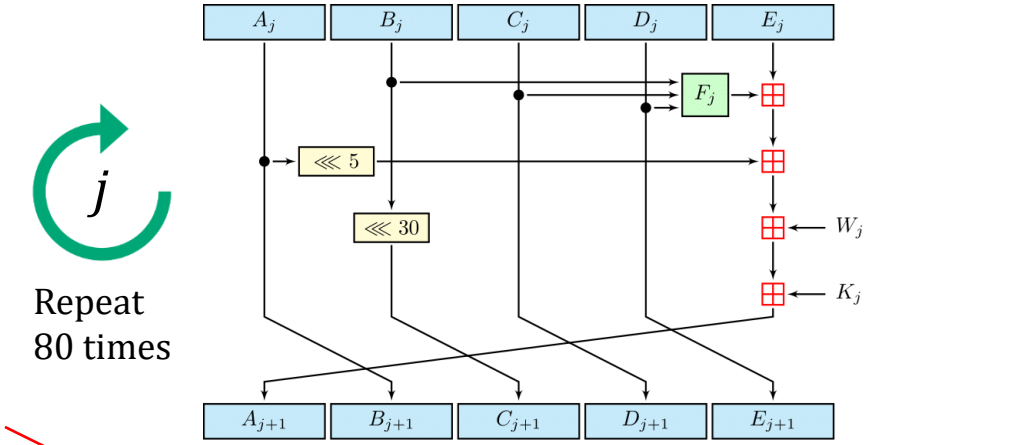
$$E : \{0,1\}^{512} \times \{0,1\}^{160} \rightarrow \{0,1\}^{160}$$

IV = 67452301 || EFCDAB89 ||98BADCFE || 10325476 ||C3D2E1F0

$E(M_i, V_i)$

$A_1 \leftarrow V_{i,1}$
$B_1 \leftarrow V_{i,2}$
$C_1 \leftarrow V_{i,3}$
$D_1 \leftarrow V_{i,4}$
$E_1 \leftarrow V_{i,5}$

for $j = 1 \ldots 16$ **do**
  $W_j \leftarrow M_{i,j}$
for $j = 17 \ldots 80$ **do**
  $W_j \leftarrow (W_{j-16} \oplus W_{j-14} \oplus W_{j-8} \oplus W_{j-3})_{\lll 1}$



Repeat
80 times

$\text{frac}_{32}(\sqrt{2})$

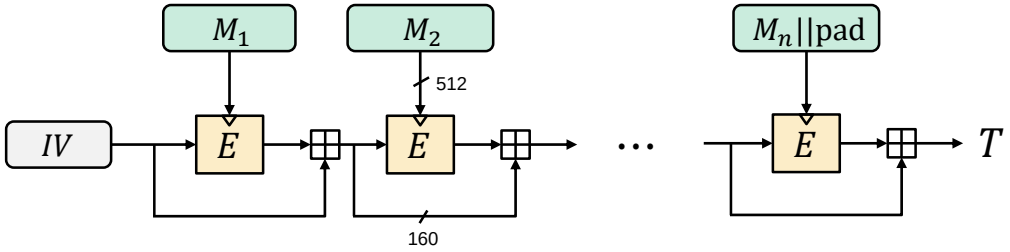
$\text{frac}_{32}(\sqrt{3})$

$\text{frac}_{32}(\sqrt{5})$

$\text{frac}_{32}(\sqrt{10})$

j	K_j	$F_j(B, C, D)$
1 ... 20	5A827999	$(B \wedge C) \vee (\bar{B} \wedge D)$
21 ... 40	6ED9EBA1	$B \oplus C \oplus D$
41 ... 60	8F1BBCDC	$(B \wedge C) \vee (B \wedge D) \vee (C \wedge D)$
61 ... 80	CA62C1D6	$B \oplus C \oplus D$

SHA0



$$E : \{0,1\}^{512} \times \{0,1\}^{160} \rightarrow \{0,1\}^{160}$$

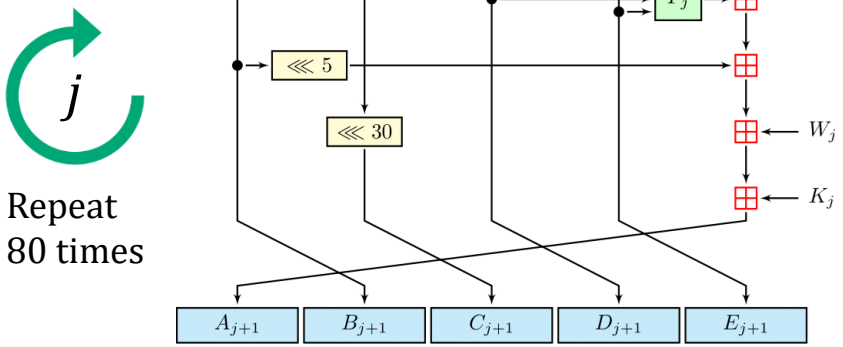
IV = 67452301 || EFCDAB89 ||98BADCFE || 10325476 ||C3D2E1F0

$E(M_i, V_i)$

$A_1 \leftarrow V_{i,1}$
$B_1 \leftarrow V_{i,2}$
$C_1 \leftarrow V_{i,3}$
$D_1 \leftarrow V_{i,4}$
$E_1 \leftarrow V_{i,5}$

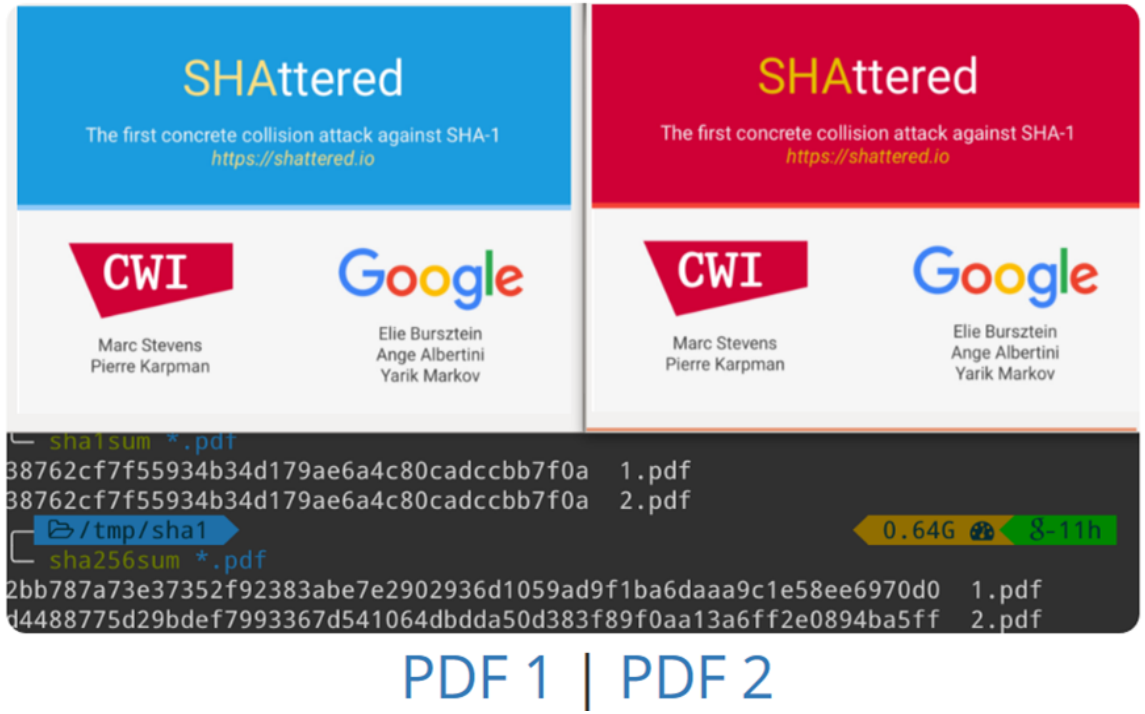
for $j = 1 \ldots 16$ **do**
  $W_j \leftarrow M_{i,j}$
for $j = 17 \ldots 80$ **do**
  $W_j \leftarrow (W_{j-16} \oplus W_{j-14} \oplus W_{j-8} \oplus W_{j-3}) \lll 1$

SHA1

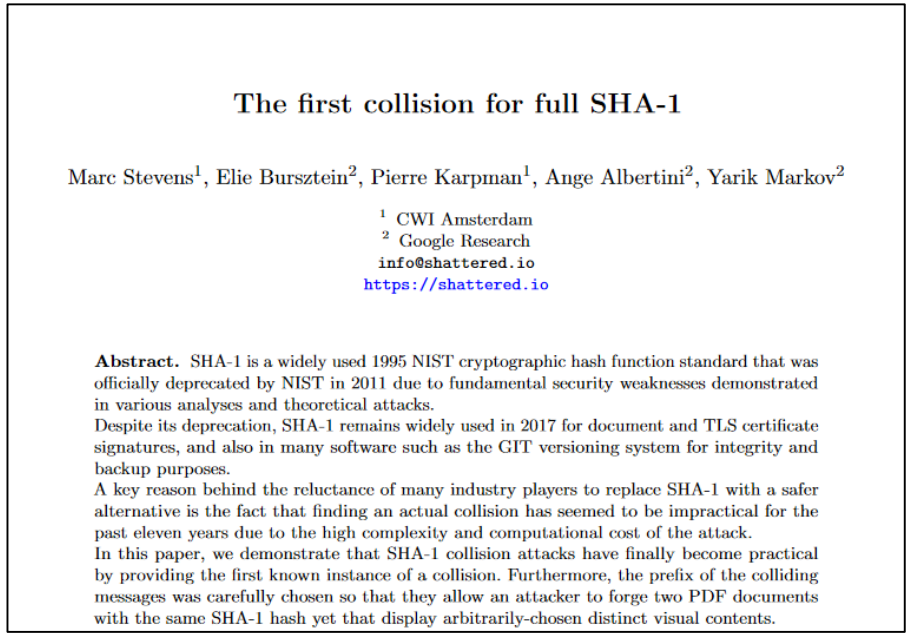


j	K_j	$F_j(B, C, D)$
1 ... 20	5A827999	$(B \wedge C) \vee (\bar{B} \wedge D)$
21 ... 40	6ED9EBA1	$B \oplus C \oplus D$
41 ... 60	8F1BBCDC	$(B \wedge C) \vee (B \wedge D) \vee (C \wedge D)$
61 ... 80	CA62C1D6	$B \oplus C \oplus D$

Attacks against SHA1



- 2004: First SHA0 collision found (Wang *et al.*)
- 2005: Theoretical attack on SHA1 (2^{69} ops.)
- **2017:** First SHA1 collision found ($2^{63.1}$ ops.) (Stevens & Karpman + Google 2017)



The first collision for full SHA-1

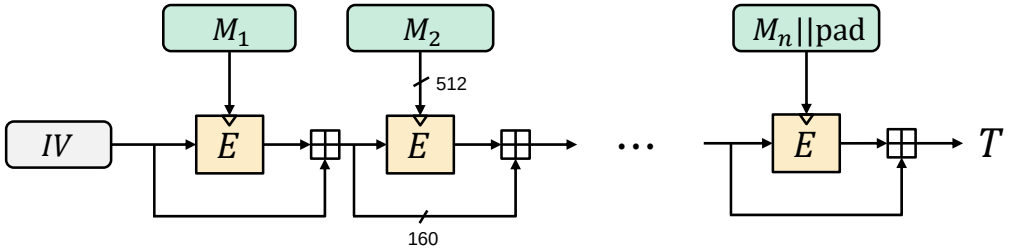
Marc Stevens[1], Elie Bursztein[2], Pierre Karpman[1], Ange Albertini[2], Yarik Markov[2]

[1] CWI Amsterdam
[2] Google Research
info@shattered.io
https://shattered.io

Abstract. SHA-1 is a widely used 1995 NIST cryptographic hash function standard that was officially deprecated by NIST in 2011 due to fundamental security weaknesses demonstrated in various analyses and theoretical attacks.
Despite its deprecation, SHA-1 remains widely used in 2017 for document and TLS certificate signatures, and also in many software such as the GIT versioning system for integrity and backup purposes.
A key reason behind the reluctance of many industry players to replace SHA-1 with a safer alternative is the fact that finding an actual collision has seemed to be impractical for the past eleven years due to the high complexity and computational cost of the attack.
In this paper, we demonstrate that SHA-1 collision attacks have finally become practical by providing the first known instance of a collision. Furthermore, the prefix of the colliding messages was carefully chosen so that they allow an attacker to forge two PDF documents with the same SHA-1 hash yet that display arbitrarily-chosen distinct visual contents.

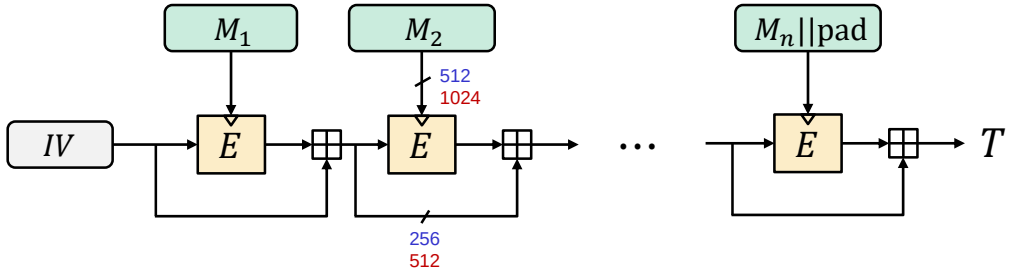
SHA2

SHA1



$$E : \{0,1\}^{512} \times \{0,1\}^{160} \rightarrow \{0,1\}^{160}$$

SHA2



SHA2-256

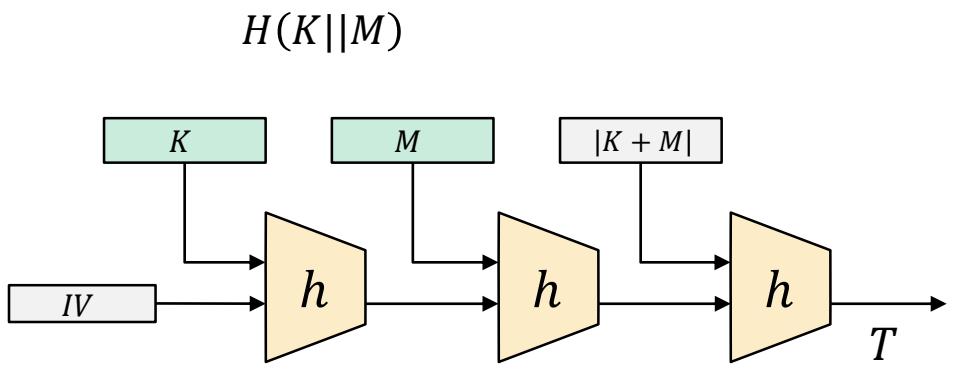
$$E : \{0,1\}^{512} \times \{0,1\}^{256} \rightarrow \{0,1\}^{256}$$

SHA2-512

$$E : \{0,1\}^{1024} \times \{0,1\}^{512} \rightarrow \{0,1\}^{512}$$

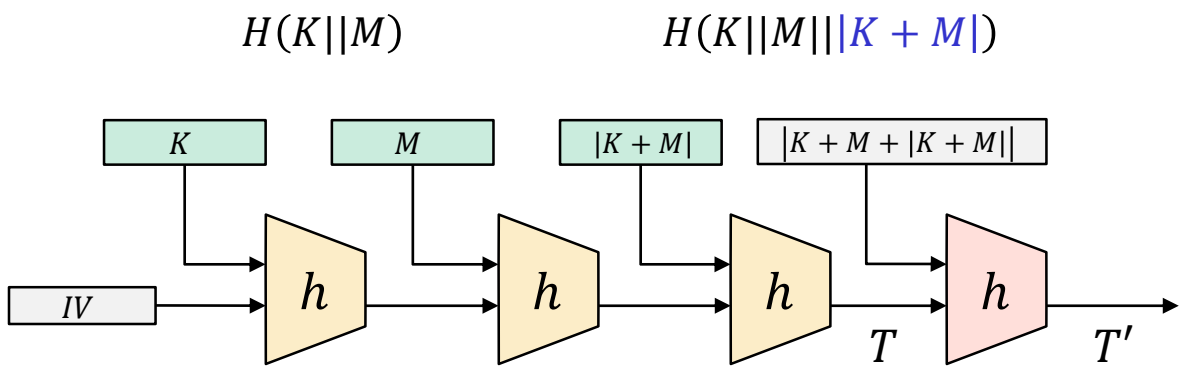
VIL-PRFs from hash functions – $H(K \,||\, M)$

- Doesn't work in general
- **Length-extension attacks** on Merkle-Damgård hash functions



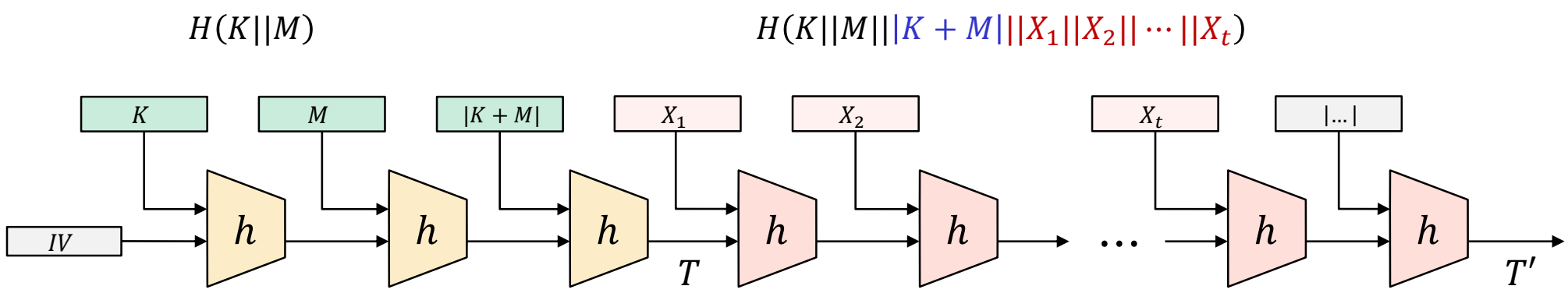
VIL-PRFs from hash functions – $H(K \,||\, M)$

- Doesn't work in general
- **Length-extension attacks** on Merkle-Damgård hash functions

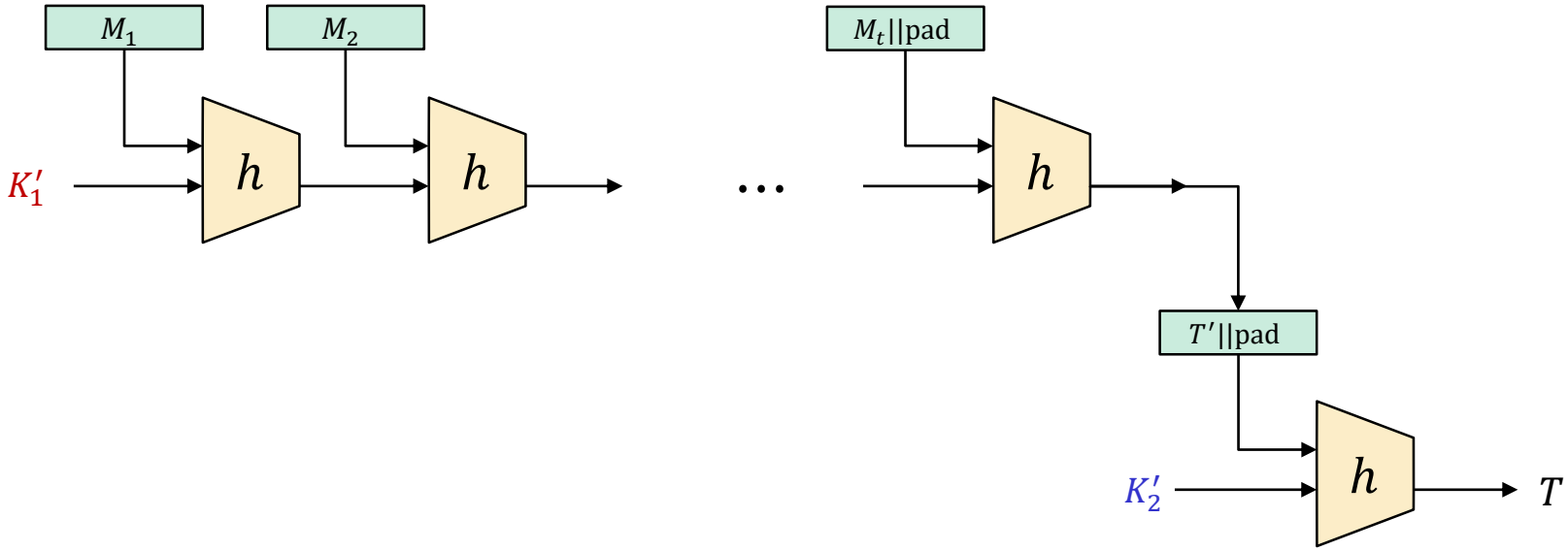


VIL-PRFs from hash functions – $H(K \,||\, M)$

- Doesn't work in general
- **Length-extension attacks** on Merkle-Damgård hash functions



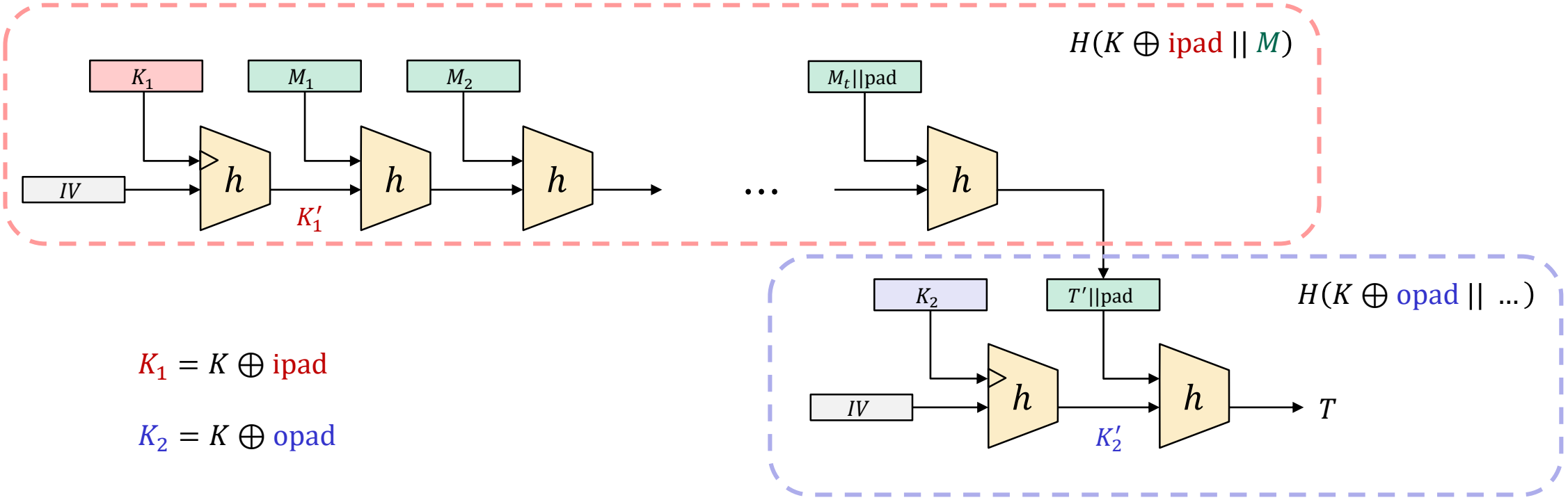
NMAC



Theorem (Gaži, Pietrzak, Rybár '2014):

If $h : \{0,1\}^n \times \{0,1\}^b \to \{0,1\}^n$ is a secure PRF then $\mathrm{NMAC} : \{0,1\}^n \times \{0,1\}^* \to \{0,1\}^n$ is a secure VIL-PRF.

HMAC



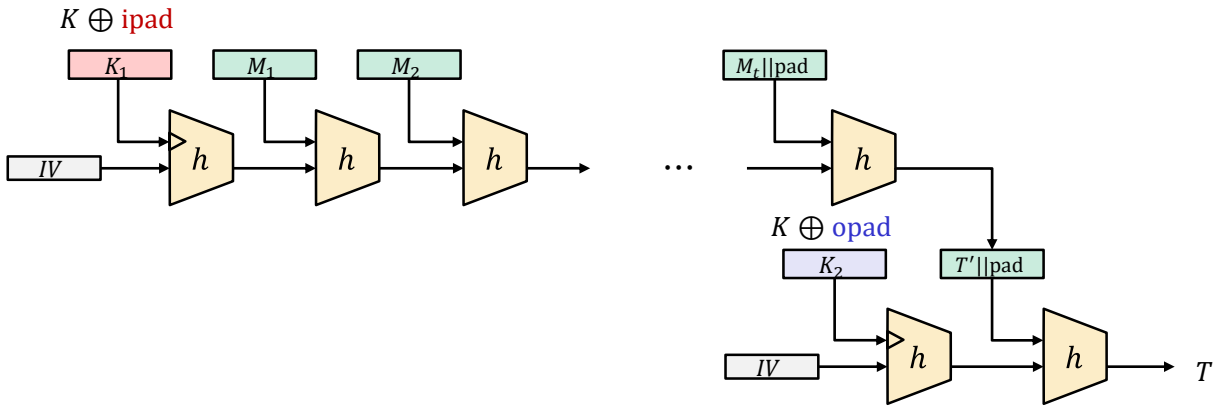
$K_1 = K \oplus \text{ipad}$

$K_2 = K \oplus \text{opad}$

$$\text{HMAC}(K, M) = H\big(K \oplus \text{opad} \;||\; H(K \oplus \text{ipad} \,||\, M)\big)$$

HMAC

- *Very* widely used
  - TLS
  - IPsec
  - SSH
  - LTE
  - …



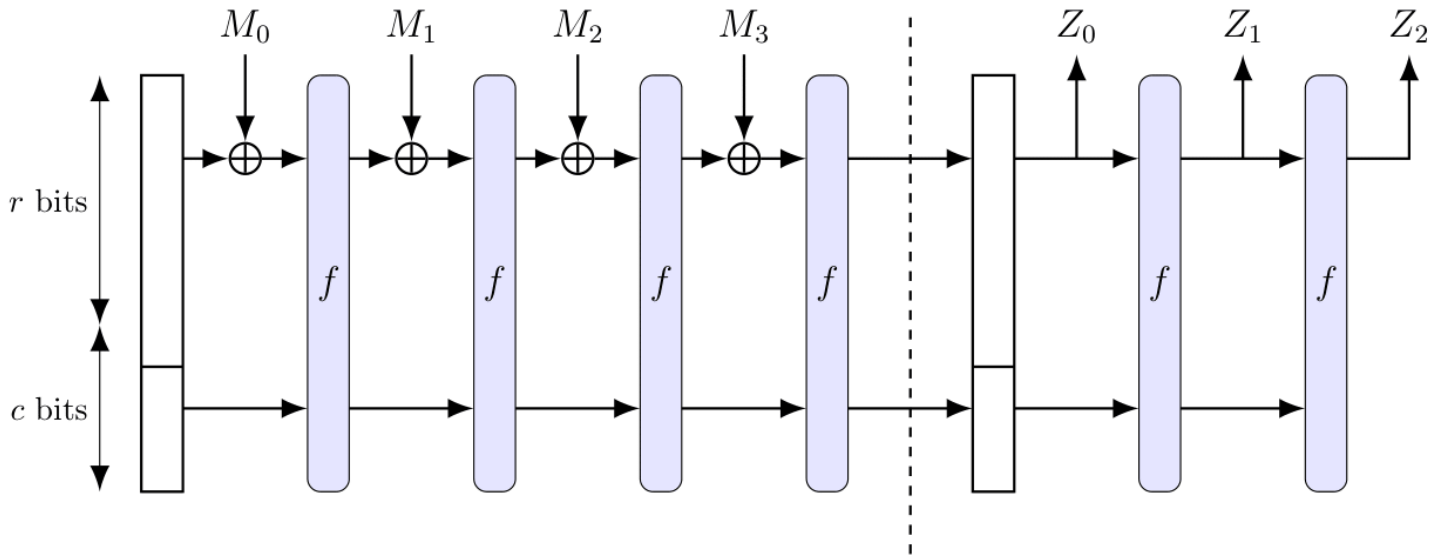
- Standardized by NIST and IETF (RFC 2104)

$$\mathrm{HMAC}(K, M) = H\big(K \oplus \text{opad} \;||\; H(K \oplus \text{ipad} \,||\, M)\big)$$

- Security proof for NMAC can be lifted to HMAC:
  - + assume h is a secure **dual** PRF (h keyed through the message is also a secure PRF)
  - + assume h is secure against **related-key attacks** (since K_1, K_2 are derived from K)
  - very tricky proof; controversies

SHA3

$f : \{0,1\}^{1600} \rightarrow \{0,1\}^{1600}$



Absorption phase

Squeezing phase